MARITIME AND MOBILE TACTICAL WIDE AREA NETWORKING (MTWAN)

Technical Guidance

ACP 200(D) Volume 2

March 2015

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP 200(D) Volume 2, MARITIME and MOBILE WIDE AREA TACTICAL NETWORKING (MTWAN) Technical Instructions, is an UNCLASSIFIED CCEB publication.

3. This publication contains Allied military information for official purposes only.

4. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD LETTER OF PROMULGATION

FOR ACP 200(D) Volume 2

1. The purpose of this Combined Communications-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 200(D) Vol 2 within the Armed Forces of the CCEB Nations. ACP 200(D) Vol 2, MARITIME and MOBILE WIDE AREA NETWORKING (MTWAN) Technical Instructions, is an UNCLASSIFIED publication developed for Allied use under the direction of the CCEB Principals

2. ACP 200(D) Volume 2 is effective upon receipt for CCEB Nations and when directed by the NATO Military Committee (NAMILCOM) for NATO nations. ACP 200(C) Volume 1 and 2 will supersede ACP 200(C), which shall be destroyed in accordance with national regulations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 200(D) Vol 2	CCEB	On Receipt	LOP

3. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals

Paul Graham

J.P. Graham
Lieutenant Commander, Royal Australian Navy
CCEB Permanent Secretary

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction And Date Time Group		**Date Entered**	**Entered by (Signature, Name, rank)**
DTG	**Correction**		

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

PREFACE

1. ACP 200(D) is one complete document combining Vol I and Vol II due to print and distribution issues and the two separate volumes should be read as a whole.

2. ACP 200(D) Vol I focus is on the MTWAN guidance and aimed at the Command, Communications Specialist (Officer and Rating), Operators and Support Engineers. It provides the baseline, scoped with the protective marking of unclassified, on how and where an MTWAN supports the Maritime and Joint environments; including the procedures and practices that are required to be understood by the Command and Operators.

3. ACP 200(D) Vol II provides the Communications Specialist and Support Engineers on how to technically provide MTWAN. This again is scoped within as much detail as can be provided within a Unclassified document. It provides the base engineering principles required to connect and enable data flows over an MTWAN which then concludes with the understanding of the Network Configuration Plan (NCP) and then the Operational Tasking Network Message (OpTask NET).

CHAPTER 1

NETWORK ARCHITECTURE

INTRODUCTION

100. Network architecture describes the logical structure and operating principles that govern a network. A Mobile Tactical Wide Area Network (MTWAN), in the maritime environment, by necessity, has a flexible logical network structure capable of supporting heterogeneous computing currently in a Radio Frequency (RF) environment which may be conducted by non RF technology as it is developed. This chapter expands upon the systems and technical concepts introduced in ACP 200 Vol 1.

AIM

101. This chapter describes proven network architectures suitable for supporting a MTWAN.

OVERVIEW

102. The term 'network architecture' is commonly used to describe a set of abstract principles for the technical design of protocols and mechanisms for computer communication. The MTWAN Network Architecture (NA) represents a set of deliberate choices from a set of design alternatives, where the choices are informed by an understanding of the requirements canvassed in ACP 200 Vol 1. In turn, this architecture provides a guide for the many technical decisions required to standardize network protocols, algorithms and schemas that appear in the subsequent chapters. The purpose of the architecture is to provide coherence and consistency to these decisions and to ensure that the requirements are met.

103. A Network Architecture describes:

a. The overall geographic layout of the network;

b. How it is connected to other networks;

c. How computers will communicate with one another;

d. How entities, such as computers and domains, are named;

e. Where security boundaries are drawn and how they are enforced; and

f. How management boundaries are drawn and selectively pierced.

DESCRIPTION

104. The illustration at Figure 1-1 presents MTWAN in terms of network topology

from an operational view and shows that a typical MTWAN consists of one or more Autonomous Systems (AS), each of which in turn comprises a collection of allied units and possibly shore communication stations all connected by a collection of backbone subnets. The MTWAN may be connected to a larger allied network.

105. Within an MTWAN, connectivity between mobile units is via Radio Frequency (RF) communications. However, connectivity from one Network Operating Centre (NOC) to another NOC, may be terrestrial.

106. In terms of topology and routing protocols, an MTWAN is influenced by its distributed and low bandwidth, high latency environment. An important key to the MTWAN routing architecture (and any routing architecture) is the design and management of Autonomous Systems.

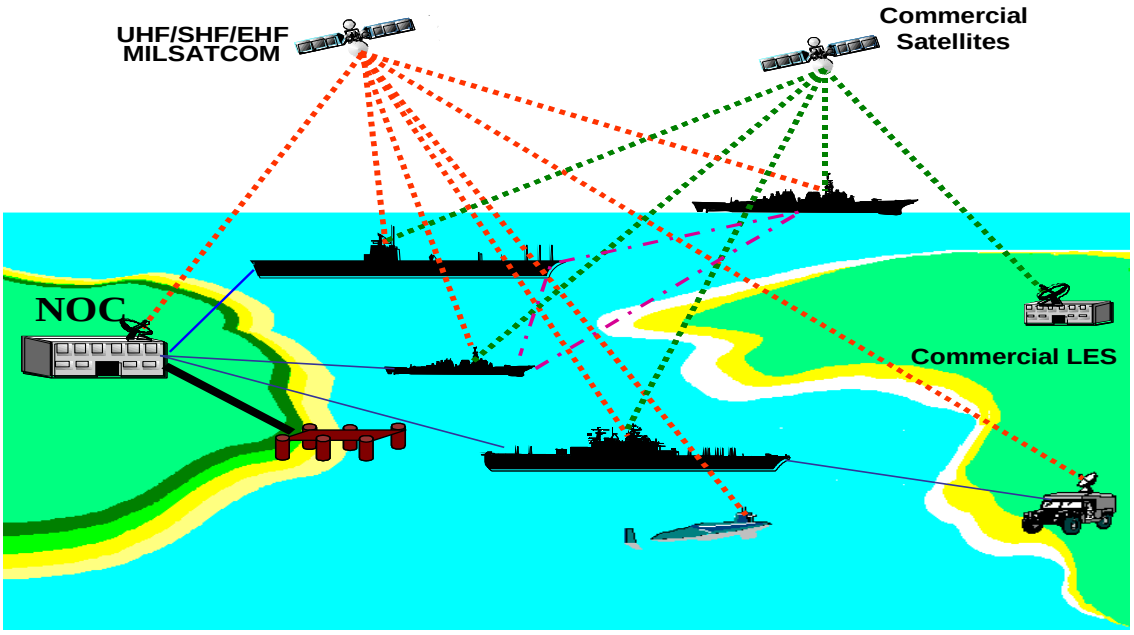

Figure 1-1 Operational View of MTWAN

107. A military tactical networking architecture must be designed to provide secure and reliable communications between the network users. Perhaps just as importantly, a military network must also be designed with flexibility. New operational requirements will evolve as well as the requirement to introduce new bearers or applications to the network. An effective architecture must be adopted to meet these changes. Internet Protocol (IP) is the universal standard for flexible networking and a prerequisite to the deployment of an MTWAN. The MTWAN is an IP network. However, it is an IP network which by necessity must integrate with a number of legacy components including radios, cryptographic equipment, and special-purpose applications. Other relevant factors that must also be understood are routing, naming and addressing, Quality of Service (QoS), and network security.

108. Military data must remain protected, therefore each node maintains at least three separate networks: an unclassified network, a national classified network and a coalition classified network. For some nations, the general purpose network of lowest classification is not unclassified but is restricted instead. The unclassified networks between two nodes from different nations may or may not be directly connected. Direct connections between one nation's unclassified network and another's classified network or between, e.g., a UK classified and an AUS classified network, may not be possible. In any case, while there is considerable information available on unclassified and classified networks, it is the networks of higher classification – national secret and coalition secret – which are used for operations. There are usually only strategic gateway direct connections between nation's national secret networks, while the coalition secret networks are usually built on shared infrastructure and can therefore be directly connected at the tactical level. The latter are the primary vehicles for information exchange in an MTWAN e.g Combined Enterprise Regional Information Exchange System (CENTRIXS) or NATO Secure Wide Area Network (NSWAN) or a Mission Secret network.

109. Figure 1-2 below depicts a typical MTWAN network architecture. Shipboard, the coalition enclave Local Area Network (LAN) connects through an access router and IP encryption device to a Wide Area Network (WAN) access router. IP encryption is needed because the classification of the transport networks is not coalition secret. From the WAN access router, traffic is further protected by link encryption before it is transmitted on the air. While operations without reach-back to shore are some times required, and one that continues to be emphasized in national and coalition communities, the majority of traffic and to and from a ship is exchanged with shore sites over SATCOM.

110. Each nation's ships are supported by a shore-based NOC. The NOC provides network and application services to their respective ships and also serves as a gateway to other users and external networks, both national and coalition. The external networks are not explicitly depicted in the Figure 1-2. The NOCs from the different nations are connected over terrestrial infrastructure. This connection as illustrated is somewhat idealized as a direct link from the coalition router at the Nation "A" NOC to the coalition router at the Nation "B" NOC. In reality, this connection may be tunneled through a variety of national infrastructures.

111. The classification used for the core transport network may vary from nation to nation and even from ship to ship within the platforms deployed from a single nation e.g. US ships typically deploy with a US secret transport core while those of the UK typically deploy with a UK classified core. (In these cases, the corresponding IP encryption device, between the appropriate LAN and the WAN access router, can be omitted.) When two or more platforms use a common core for WAN transport, the platforms can be connected directly over Line of Sight (LOS) or Beyond Line of Sight (BLOS) links as shown in the figure below. The case of most interest for the coalition is that of a Cipher Text (CT) core, commonly known as a Black Core, i.e. one in which all user traffic is

encrypted on the core. Many nations are converging on CT core architectures in order to have more flexibility in operations with coalition and joint forces. More details on CT core are provided in the network security chapter.

112. Direct ship-to-ship connections between MTWAN participants are achieved by directly connecting LOS/BLOS bearers to the coalition access routers on the platforms. These connections are the bottom-most of the ship-to-ship connections illustrated in Figure 1-2. Even with a common core, direct links may be deployed for reasons of expediency or efficiency.

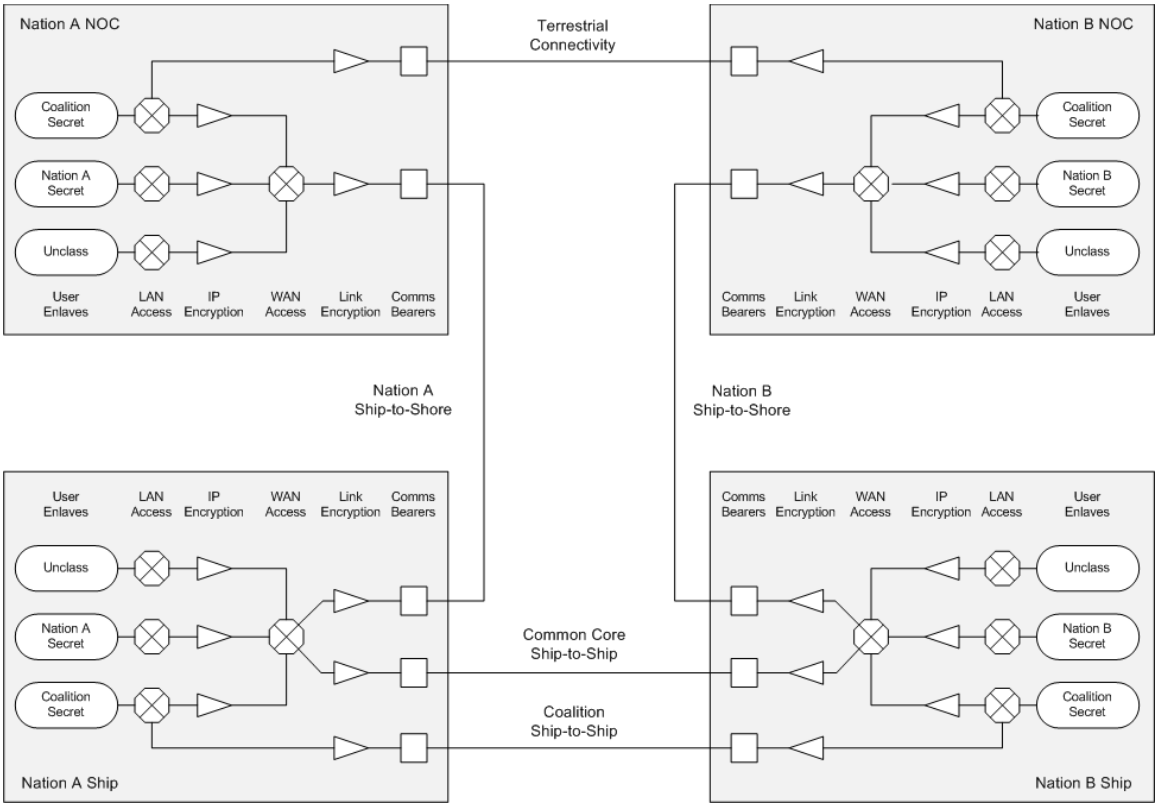

Figure 1-2 MTWAN Network Architecture

113. The satellite and LOS/BLOS bearers employed for tactical communications are limited in bandwidth, higher in latency, and more error-prone than communications links used in terrestrial networks, and they are prone to intermittent connectivity. Even in benign environments, ships move into and out of LOS and BLOS range, satellite antennas are subject to blockage, propagation can be problematic, and electro-magnetic interference (EMI) must continually be guarded against. The realities of communications challenges at all times drive architectural decisions. Networking protocols such as routing must be light-weight and adapt quickly to changes. QOS is needed to prioritize

mission critical traffic when not everything can be serviced. Applications should avoid excessive chattiness and should continue to function even when connections to shore are lost.

114. Data placed on the coalition secret network is deemed releasable to all the nations participating in that network. Since at any one time there are likely to be multiple coalitions engaged in different operations, there are multiple coalition networks e.g. All coalition partners may be on the CENTRIXS GCTF network, however, an individual alliance such as AUSCANNZUKUS may have an additional network within the same CENTRIXS architecture.

115. A cross-domain solution (CDS) can be used to move data from one enclave to another in an MTWAN. Data may be moved with relative ease from low to high, e.g. from unclassified or restricted to coalition secret or from coalition secret to national secret. Although the availability of such devices in a tactical environment may be limited, this may be done automatically with data diodes. When appropriate, it is also possible to move data from high to low, e.g. from national secret to coalition secret. However, moving data from high to low is relatively difficult. Guards such as Radiant Mercury which do this automatically require the data to be precisely formatted so that it can be checked against a configured rule set with the development of agreed accredited rule sets difficult. Guards for unformatted data require manual transfer or a reliance on technology that is very challenging to security accreditation. It should be noted that while it may be possible to automate data transfer, the examination and ultimate approval for release is a command function conducted by a human operator. The most time-tested CDS is the old-fashioned "sneaker-net" in which data from one enclave is copied to removable media such as a CD and then hand-carried to a terminal on the other enclave. The bottom line is that guard technology is cumbersome. Guards must be employed judiciously if a network architecture is to be effective.

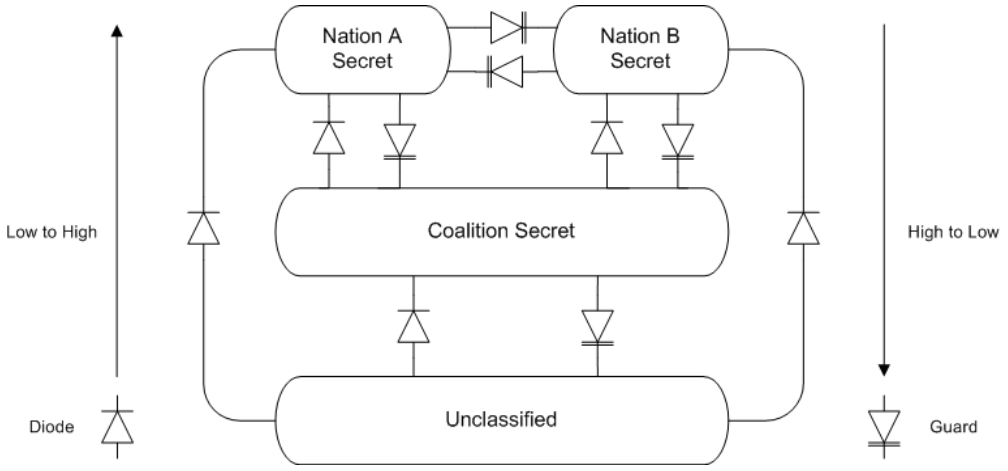

Figure 1-3 Cross domain data transfer in a coalition networking environment

116. The existence of multiple enclaves can have a significant operational impact

depending on where operators will actually conduct the business of warfighting. The particular question is whether business is first conducted on national secret networks (e.g. US SIPRNET) and then releasable data passed down to the coalition network, (e.g. one of the CENTRIXS enclaves) or whether it is conducted first on the coalition network to start with then passed by diode to the national network. This factor needs to be understood in the conduct of an operation and required information flows to support the number, location and fitting of the right amount and type of user access devices (UAD) onboard a platform.

117. Historically, in US-led operations the Common Operational Picture (COP) has been prepared on US Global Command and Control System (GCCS) then released through Radiant Mercury guards to the coalition network. Coalition contributions to the COP have had to be first released through national situational awareness reporting over national networks and strategic gateways to be fused and then reported to that coalition network COP. This is a good example of warfighting being conducted on a network other than the coalition and then being released to the coalition network for wider dissemination.

118. All significant military operations are executed by multi-national coalitions supported by a Coalition Network, therefore a standard suite of Joining Management and Exit Instructions (JM&EI) are maintained and agreed by all the principal coalition partners. The coalition network will always share existence with the national secret networks, therefore these STANAGs and associated processes should be carried through from one network to another to assist the information exchange requirements of the operators.

119. In Afghanistan, operations with the US, UK, and other NATO nations revealed difficulties with conducting multi-national missions using different national networks and then trying to communicate between nations through guards. The Afghanistan Mission Network (AMN) was born out of this need (2008-2009) and was deployed as the primary C4ISR network for all International Security Assistance Forces (ISAF).

120. The AMN supports the transfer of email, web browsing, blue force tracking, VoIP, and VTC. As the AMN was stood up, 165 applications were moved to it, 55 of which were considered critical. The AMN consists of an ISAF secret core provided by NATO with various national extensions, e.g. CENTRIXS-ISAF for the US, Overtask for the UK, and Land Combat Support System (LCSS) for Canada. The process for the validation and assurance of the information flows, training, tactics and procedures (TTP) is conducted by the Coalition Interoperability Assurance and Validation (CIAV) organization, which is being conducted in support of the development of JM&EI for all future mission networks e.g. NATO Future Mission Network (FMN) or US Multi Partnering Environment (MPE).

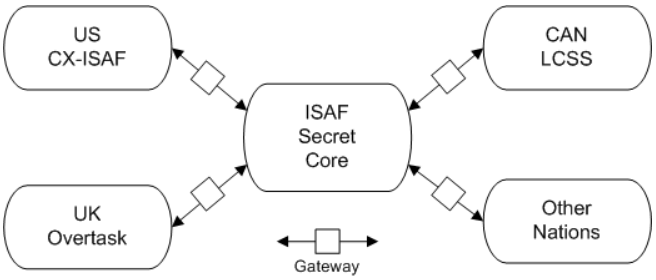

Figure 1-4 Afghan Mission Network

121. There are no guards in the AMN architecture. The gateways between the AMN core and the national extensions may include firewalls, intrusion detection and prevention devices, and other network devices, but no CDS; the entire network is run at a common security level.

122. Evolution of the future mission network concept is the US provision of the Global Information Grid (GIG) 3.0 which will underpin all US MPE network provision. This proposal, which is also aligned to the US Joint Information Architecture (JIE), is to reuse CENTRIXS Global Counter Terrorism Force (GCTF) as a global coalition Cipher Text Common Mission Network Transport (CMNT) network. Through the CMNT would be tunneled classified networks, including coalition networks such as CENTRIXS Coalition Maritime Forces Pacific (CMFP) and national secret networks such as US SIPRNET, called Operational Network Domains in the GIG 3.0 architecture. These would be separated by high-grade IP cryptological devices. The classified networks would be further partitioned using commercial-grade virtual private network (VPN) technology into potentially ad hoc user communities of interest to support operational missions as needed, a construct GIG 3.0 calls Agile Virtual Enclave (AVE). The concept of operations is that an AVE would be stood up and managed by an operational commander to support a specific mission, a concept very much aligned with NATO FMN and US MPE. Due to each AVE being separated by VPN equipment, that are not cryptographically controlled, the operational commander is afforded more flexibility in the admission of potential partners to the enclave. An AVE could also span multiple classified networks, through the use of approved and accredited cross-domain devices.

123. The AUSCANNZUKUS community is currently developing the federation of their own national secret networks with a strategic gateway that can enable direct operational communications. This initiative, known as PEGASUS, is initially replacing the current GRIFFIN infrastructure but has the reach to repurpose AUSCANNZUKUS requirements across CENTRIXS and SIPR REL. Phase one initially only provides strategic email with attachments across the shore facilities but is being rapidly developed to connect national systems fitted in operational platforms. This is significant and relates to the Future Mission Network concept by the standardization of guards and services in the architecture and by federating national secret rather than mission secret networks. This concept could form the basis of any high trust core coalition network.

CHAPTER 2

MTWAN BEARERS AND SUBNETS

INTRODUCTION

201. A MTWAN is a collection of subnets (short for "subnetworks") that are connected to each other through routers that in turn are connected by the various communication paths available to a tactical user. In the context of IP networking, a wire, optical fiber or an RF bearer, together with its associated interface and cryptographic equipment, form a subnet that connects two or more routers together.

202. Unlike terrestrial networks where subnets are connected by copper or fiber pathways, the deployed tactical military environment is typically a very mobile one, where non physical communications bearers are the only paths available to move data between geographically dispersed networks. These communication paths have unique and often restrictive characteristics that impact on the effectiveness of exchanging IP traffic. Capacity and connection integrity are always an issue with RF paths and performance limitations are often necessary to achieve reliable links.

AIM

203. This chapter provides an overview of communication bearers and subnets and their utilization within an MTWAN.

OVERVIEW

204. A typical MTWAN is formed between geographically dispersed platforms with single/multiple LANs connected to one another through the use of disparate communication links. Common wireless communication bearers such as UHF SATCOM, 3G, UHF and HF connect physically remote routers through the use of the first three layers of the Open Systems Interface Model (OSI) which is illustrated at Figure 2-1.

205. The end state is to achieve a reliable LAN-to-LAN connection to enable the exchange of IP packets at sufficient speeds and volumes to deliver acceptable application performance.

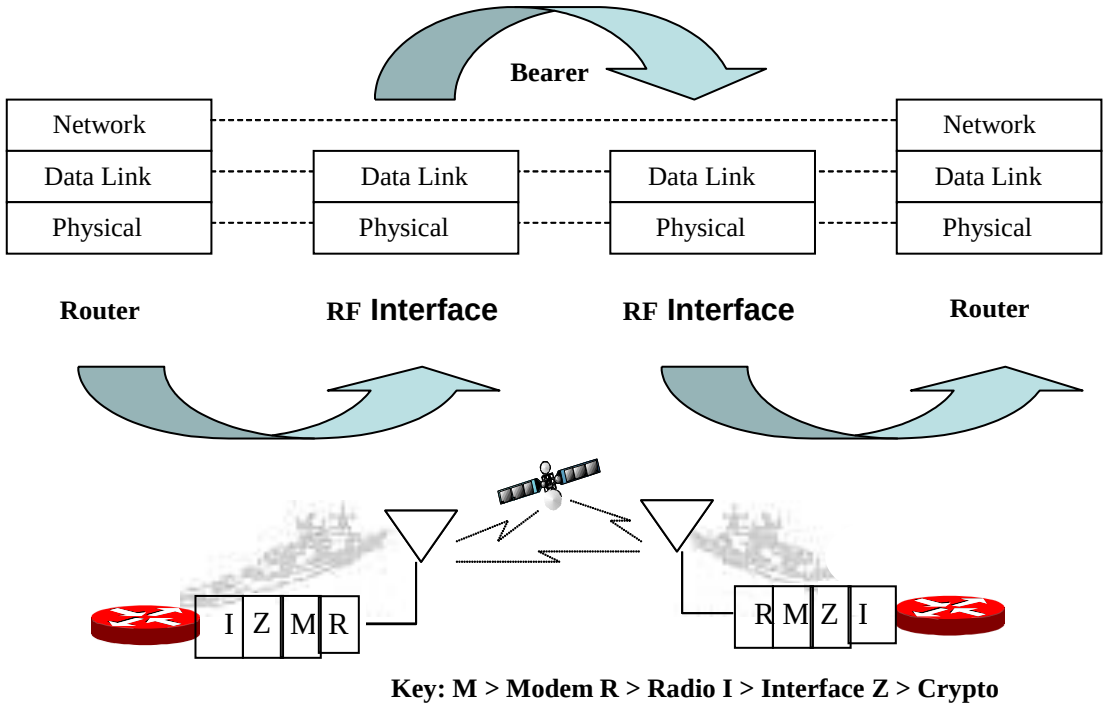

Figure 2-1 Communication Subnet(s)

COMMUNICATION BEARERS

206. IP was designed around a land-based communications infrastructure that is built on highly reliable, wideband and low-latency transmission media such as copper wires or optical fibers strung between endpoints, providing sustained, two way connection over extended periods. An MTWAN, however, relies on wireless bearers of various forms including duplex, half-duplex and point-to-multipoint for example, limited by the number of radios and radio frequencies available and often of short or limited duration. Full-duplex point-to-point bearers (such as ISDN, INMARSAT) can interface directly to routers, however, interface equipment is usually required to facilitate connection between routers with standard Serial or Ethernet interfaces over tactical RF bearers.

207. The characteristics of the bearer in question (i.e. whether it is half-duplex or full-duplex, whether it is broadcast or non-broadcast and whether it is a high-latency circuit over a satellite) will determine the interface technology.

TERRESTRIAL BEARERS

208. The typical terrestrial bearer is an Integrated Services Digital Network (ISDN) which is a set of protocols that allow the user to fully integrate voice and data services over a single communication telephone line. ISDN lines are normally leased from the local telecommunication service provider and can provide a dedicated full-duplex, fixed point-to-

fixed point link for digital network communication. ISDN lines are typically used as a means to provide connectivity between fixed land-based units such as Communication Stations and shore-based NOCs. As ISDN is a public data network, information transmitted over ISDN must be protected with a Type 1 encryption device. Other shore based, fixed infrastructure networks can also be used to interconnect fixed sites and can offer higher capacity and increased reliability over historic switched networks.

MILITARY SATCOM

209. A satellite system that is used for the provision of purely military services that is operated and / or owned by the military or government contracted personnel. The service offers a high resilience and tolerance to interference and attack and is designed to be respond to rapidly changing military priorities. National Governments and Military Authorities have Memorandums of Understanding (MOU) in place in order for individual nations to use the services or bearers of other National Military SATCOM systems.

COMMERCIAL SATCOM

210. INMARSAT is a commercial satellite system used for voice and up to 500 kbps data connectivity. The system uses geostationary satellites to provide near global coverage for maritime and land force elements. Because it uses geostationary satellites the connection has a high latency, which makes it less efficient for TCP. Regardless, it has been extensively used by nations to provide reachback connectivity between mobile units and shored-based NOCs. As a commercial satellite system the expense of this connection can be prohibitive. To limit budget over-runs and provide fixed costs many nations lease dedicated INMARSAT channels or acquire large blocks of data throughput.

211. The information exchanged between any two network nodes traverses a variety of communications links such as the legacy INMARSAT B system, Broadband Global Area Network (BGAN, an IP-based service provided by INMARSAT), commercial and military SATCOM, radio nets, mobile broadband and the Internet. The information may also need to traverse multiple hops before reaching its destination. Information carried by these systems is accessible by the public and therefore the confidentiality and integrity of the information is at risk. Crypto security will be provided for IP traffic leaving an MTWAN node and traversing untrusted communications systems to get to its final destination or its next hop.

HIGH FREQUENCY GROUNDWAVE

212. HF EBLOS uses the HF ground wave to provide data connectivity between MTWAN units. The high Bit Error Rate (BER) and narrow bandwidth limit this connection to relatively low data rates. However, this may provide a viable solution for disadvantaged units with low Information Exchange Requirements (IERs). Several technologies have been employed to provide ELOS solutions although no nation has yet adopted this as a primary network connection between mobile units.

HIGH FREQUENCY SKYWAVE

213. Various investigations have been conducted in order to provide a viable HF BLOS solution. HF BLOS subnets use skywave RF links to provide connectivity. As such, these types of connections are generally point-to-point solutions with very low data rates. The high BER of HF makes this type of channel unsuitable for TCP connectivity. Various techniques have been developed to improve this, however, as yet no deployable HF BLOS solution exists.

LINE OF SIGHT

214. Line of sight (LOS) is a type of propagation that can transmit and receive data only where transmit and receive stations are in view of each other without any sort of an obstacle between them. UHF Radio and VHF Radio are examples of LOS communications.

Bearer	Link Rate	Typical Use	Subnet Characteristics
ISDN	2048 kbps	Used while units are alongside or for trunk communication between NOCs. May solve land based point-to-point connectivity requirements	Full-duplex, point-to-point Low latency
Wideband SATCOM in Q, Ka, Ku, X bands	Varies widely but typically 1.5 to 10 Mbps+	Long range reach back to national operations centres. Primary, high capacity IP transport	High reliability, high capacity, full or asymmetric duplex, long lasting. Some feature MIL protection. Long path delay, high relative cost
Free Space Optics (FSO)	2 Mbps – 10 Gbps	Short to medium range. Can be laser or Light-emitting diode technology. HD, Email Chat, COP, High Data Rate DCP, Range finding	Relative new technology that is currently only used for military niche capability but is increasingly a contender for mainstream bearer for C4ISR.
Commercial SATCOM Fleet Broad Band (FBB) - L Band e.g. INMARSAT	up to 432 kbps	Long range reach back to national operations centres. Secondary, medium capacity IP transport	High reliability, high capacity, full duplex, may be long lasting or limited duration. Commercial provider, near global coverage. Long path delay, very high relative cost
HF Wideband	Up to +48kbps depending on BW available	Email, Chat, COP, Low data rate DCP	Long range Skywave propagation dependent on atmospherics, etc
HF Groundwave (narrowband)	4.8-9.6kbps (SSB)	Email, Chat, COP, Low data DCP	HF Surface Wave, Ranges of 200-300Nm achievable.

			Increased data rates achievable with ISB
HF Skywave (narrowband)	4.8-9.6 kbps (SSB)	Email, Chat, COP, Low data DCP	HF Skywave, Ranges of 2000-3000 Nm achievable. Increased data rates achievable with ISB
UHF SATCOM 25kHz	up to 48 kbps	Low data rate IP applications like Email, Chat, Low data rate DCP, COP	High reliability, low capacity, wide coverage , moderate cost, limited availability
UHF SATCOM 5 kHz	up to 9.6 kbps	Very low rate applications like Email, Chat, COP	Very low capacity, wide coverage, moderate cost, wider availability
4G	20 Mbps +	Very low rate applications like Email, Chat, COP	Military use of commercial bearers and military 3G nodes
3G	2 Mbps	Very low rate applications like Email, Chat, COP	Military use of commercial bearers and military 3G nodes.
VHF/UHF LOS	up to 1.92 Mbps (depends on available bandwidth, typically 2.5x BW	Email, Chat, DCP, COP, non-constant bit rate traffic.	Limited to LOS (UHF ~20 Nm, VHF ~80 Nm)

Figure 2-2 Communication Subnets Matrix

SUBNET TECHNOLOGIES

215. Subnet relay is the use of tactical wireless bearers to provide Wide Area Network capability over IP based networks. This network may or may not be connected to a single or multiple satellite bearers to provide reachback to Network Operating Centres (NOC) and Data Centres. Alternatively, the entire network may be "NOC-less" and operating in a tactical bubble which is particularly relevant to maritime or rapidly deployed joint expeditionary forces.

216. Various subnet technologies can be employed in an MTWAN to provide IP connectivity over tactical wireless bearers. They are intended to provide a multi-node, multi-hop, mobile-to-mobile IP connectivity over FSO/VHF/UHF LOS and HF ELOS. Relay between nodes is used to extend the coverage of a subnet beyond a single hop. A subnet is a segment of a data network connecting two or more network devices, a network within a network that operates at Layer 3 of the OSI model. Subnetting is the division of a network into smaller networks (subnets) with the supporting communications bearer, at Layer 1 of the OSI model, able to pass IP data.

217. Maximising the use of all available bearers within the task group provides a feasible alternative to SATCOM, and forms a communications backbone for the MTWAN. UHF LOS and HF ELOS are bearers available on most naval platforms, while VHF LOS and HF BLOS provide useful additions.

218. SNR is most easily explained with a few scenario diagrams where ships are not all within LOS. The scenario that will be considered is that of two battle groups where a ship moves from one battle group to the other. The scenario is depicted through Figures 2-2 – 2-7. The notion of relaying is depicted in Figure 2-2. This figure illustrates a ship (red ship to the left) wanting to communicate with another ship (red ship to the right) within the same battle group but beyond its line-of-sight (black circles). Since direct communication is not possible, the ship originating the traffic will call upon another ship, a relay ship (blue), which is within LOS communications of the source and destination ships to relay the information.

219. Each ship within the battle group becomes aware of those ships it can reach directly and those it can reach via relay(s). Thus, all ships within this task group automatically form a single SNR (self-configuring) subnetwork.

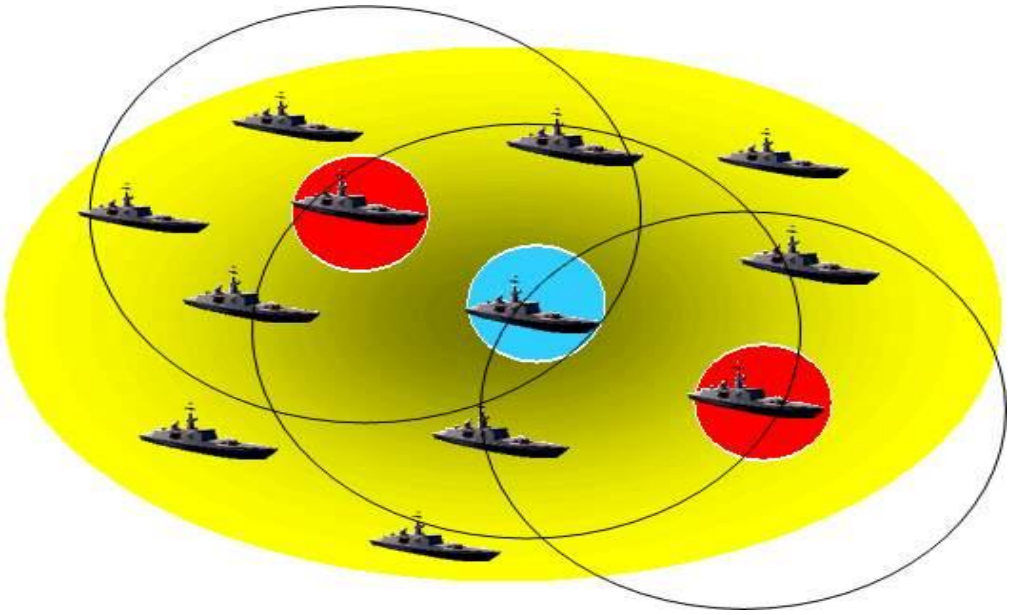

Figure 2-3 Relaying Concept

220. Figure 2-3 merely illustrates that a ship is moving from one task group to another task group. During the move, it will continue to communicate with members of the task group.

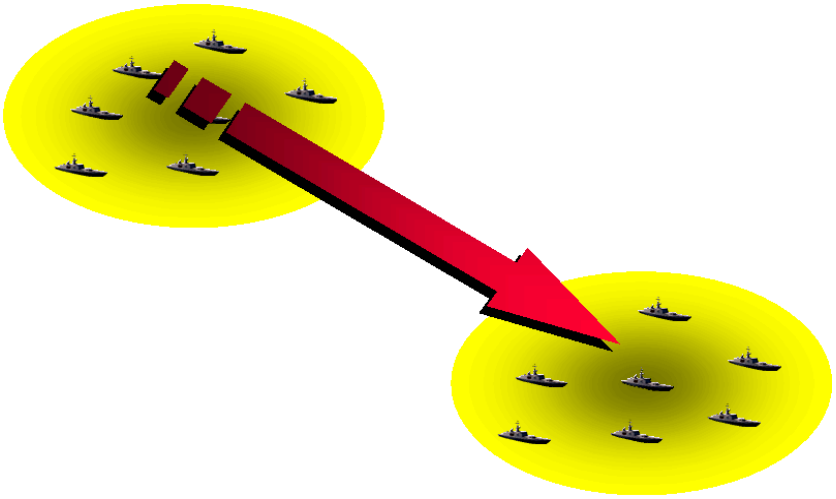

Figure 2-4 Ship Moving from one Task Group to Another

221. Figure 2-4 illustrates that as the subject ship is moving toward the other task group, it may change its relay ships. In this example, the moving ship has moved outside of direct communication with the ship it was using as a relay before and, therefore, picks another ship that is in contact with him as the relay point. This illustrates that the subnetwork is dynamically updating its relay architecture as the ship's move. It is also shown that the ship can use other ships as relay, as appropriate, to reach other ships within the Task Group. Any ship can have more than one relay and relays are picked up dynamically.

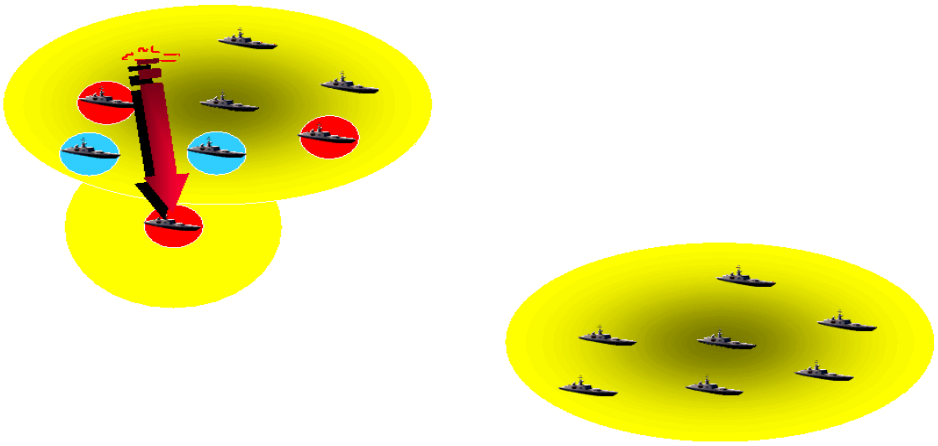

Figure 2-5 Multiple, Dynamic Relays

222. As the ship is moving toward the other Task Group, it may find itself within LOS communication range from another ship. In such a case (Figure 2-5), the two ships can communicate directly, without the need for a relay ship.

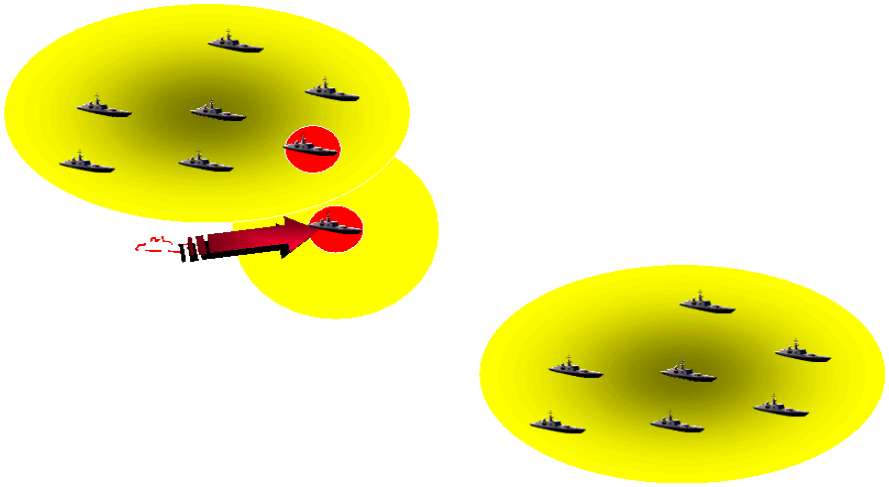

Figure 2-6 Relaying only when needed

223. As the ship continues to move away from its initial battle group, it may find itself outside of communication range from any ships in either of the two Task Groups. In such a case (Figure 2-6), the subject ship will be de-affiliated from its initial battle group SNR subnetwork, and the ship will form its own SNR subnetwork.

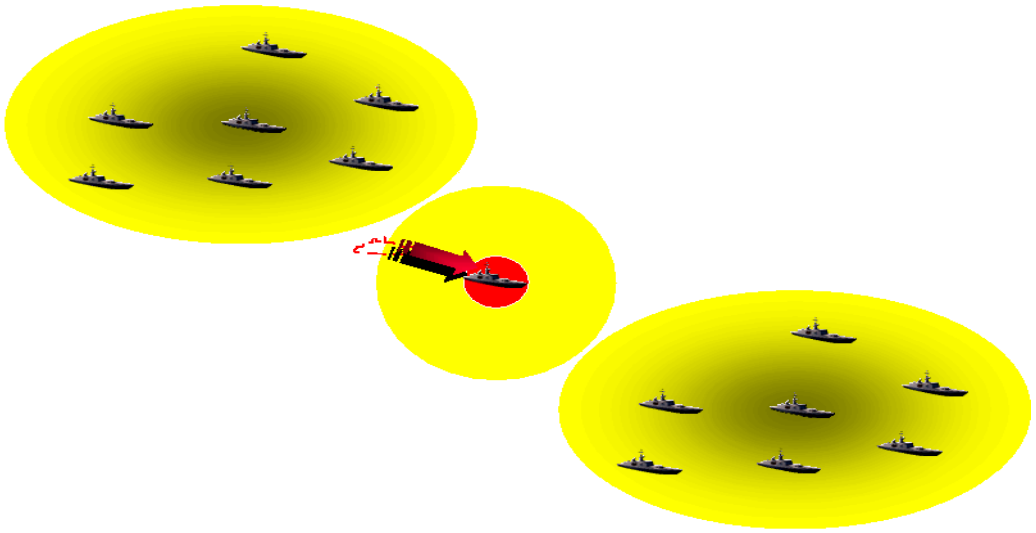

Figure 2-7 Subnetwork Splitting

224. Eventually the ship arrives within LOS communication range of the other Task Group. At that time, the two SNR subnetworks (single ship and second Task Group) will merge to form a single SNR subnetwork (Figure 2-7). As before (Figure 2-6), the ship can communicate directly, without relay, with other ships within LOS.

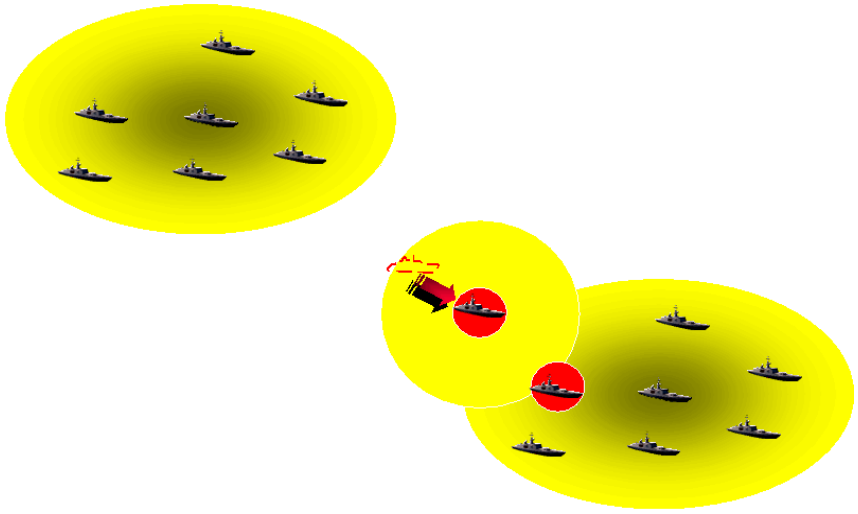

Figure 2-8 Subnetwork Merging

225. Figure 2-8 illustrates that in this new Task Group, multiple relays may be required from source to destination.

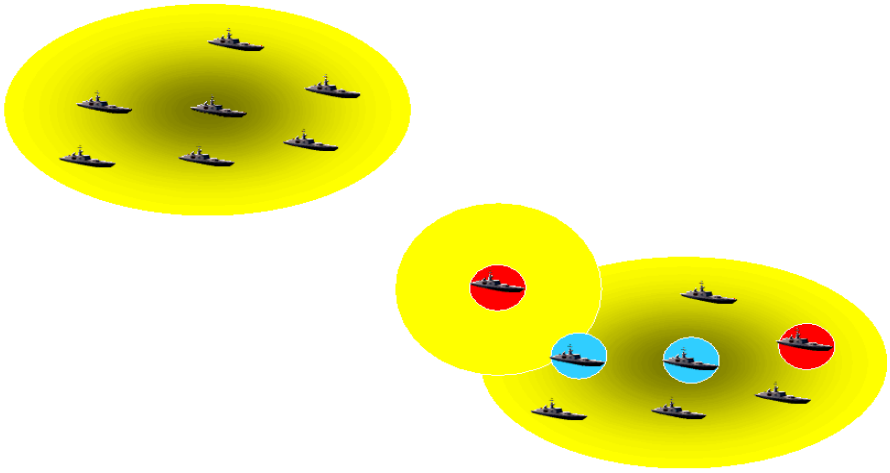

Figure 2-9 Multiple Relays to Destination

MTWAN SNR CAPABILITIES

226. Current fielded and tested CENTRIXS Subnet Relay technology limits the tactical LOS and BLOS network to 16 users (platforms), with the maximum number of relays being 4 (allowing 5 hops, which will cover approx 100 Nm in a straight line assuming 20 Nm LOS distance, or more than a 1000 Nm for HF ELOS). A typical network would have fewer platforms and be less geographically dispersed.

227. A generic MTWAN SNR network will be capable of fully distributed (e.g. masterless) and automatic operations across limitless platforms and relays.

228. An MTWAN SNR network will be capable of allocating bandwidth in proportion of each platform's instantaneous traffic load.

229. SNR is a self-configuring, self-organizing network technology. Current SNR technology reconfigures within 2-3 minutes when a UHF link or many links are lost, or when a new link (new member) appears.

230. SNR will be capable of supporting medium bandwidth applications such as DCP, COP dissemination, web browsing, FTP, email with attachments and be capable of supporting more bandwidth intensive applications if faster communication links are provided.

231. SNR will allow for bulk encryption at the Link Layer. The encryption strength will be dictated by the cryptos used in conjunction with the SNR system. SNR will be capable of interfacing to national cryptos used in AUSCANNZUKUS nations.

232. Current SNR will achieve coded data rates of 2.4 kbps to 16 kbps using HF ELOS (SSB) with high speed HF modems. In the future, higher data rates could be achieved using new waveforms, ISB radio, or multiple non-adjacent HF channels.

233. SNR will achieve coded data rates of 16 kbps to 96 kbps using UHF LOS over a standard 25 kHz audio frequency interface channel. Using an intermediate frequency (IF) channel, on radios that support this function, coded data rates of 384 kbps to 1.92 Mbps using 100kHz, 300kHz and 500kHz of contiguous UHF bandwidth, can be achieved.

234. SNR will provide the capability to manually initiate and terminate relays (used in an EMCON managed environment).

TECHNICAL LIMITATIONS AND INITIAL ASSUMPTIONS

235. A number of design parameters were provided by AUSCANNZUKUS for the design of an SNR system. In addition, to the items listed in the previous section, they are:

236. There are a limited number of radios available onboard sea-going units, therefore subnets will probably be limited to a single radio/frequency. A SNR system will be capable of operation when untethered (mobile) platforms have a single half-duplex radio per subnet;

237. All nodes (platforms) are mobile, therefore relay platforms must be selectable automatically and dynamically;

238. Reliable and unreliable link operations must be supported;

239. A subnet will be made up of bearers of a single nature (e.g. all HF BLOS, all UHF LOS etc);

240. Platforms have access to a reliable clock; and

241. Tx/Rx switching times of the order of 20 ms using HF and 50 ms using UHF are expected of current naval radios.

242. Many of these assumptions restrict the performance of SNR and do not apply if modern radio equipment with extended bandwidth access, fast switching ,etc are used. Application performance will likely drive future implementations of SNR to these modern radios.

HIGH FREQUENCY INTERNET PROTOCOL (HFIP)

243. HF IP provides IP forwarding over a HF data communications system. The system is based on STANAG 5066 and uses a modified Token Ring protocol as a media access control protocol over a shared broadcast HF channel. HF IP also provides dynamic routing based on the OSPF routing protocol.

244. HF IP supports multi-node IP networking over the air at data rates up to 9600 bps for single sideband and up to 19200 bps for two independent sidebands. Data rates are dependent on propagation conditions, distance and equipment.

245. The system is intended for use with surface wave paths which provide Extended Line Of Sight (ELOS) coverage of up to 200 nm at sea. However, it can be used to support Beyond Line Of Sight (BLOS) using sky wave with proper selection of frequency, antenna and data rate.

246. HF has traditionally been used for low data rate communications, often in a broadcast manner, in which broadcast transmissions will be received by many stations at the same time.

247. With current modem technology, HF can support data rates over the air of up to 9,600 bps over Upper Side Band (USB) operations and up to 19,200 bps over Independent Side Band (ISB).

248. Commercial implementations based on STANAG 5066 Edition 1.2 support Simple Mail Transfer Protocol (SMTP) E-mail or IP forwarding using the Carrier Sense Multiple Access (CSMA) protocol to allow multiple nodes to share a half-duplex and single channel. The CSMA protocol is simple to implement, but very inefficient as the data throughput suffers from retransmissions due to collisions.

249. The Token Ring protocol established in STANAG 5066 Edition 3 provides a more efficient media access protocol for multi-node ad-hoc networks, in comparison with CSMA. The protocol is distributed as there is no master-slave relationship between nodes, and nodes can join and leave at any time.

250. HF IP provides a means to forward IP traffic over a HF data communications system comprising modems, transmitters, receivers, power amplifiers and antennas. Figure 2-8 shows a typical network configuration of a node that makes use of HF IP. The installation of an HF

IP system consists of an HF IP Interface, known as RF Controller, a link crypto, an HF modem capable of supporting ISB, and HF radio equipment. The figure also shows other communications subnets to which the node can be connected.

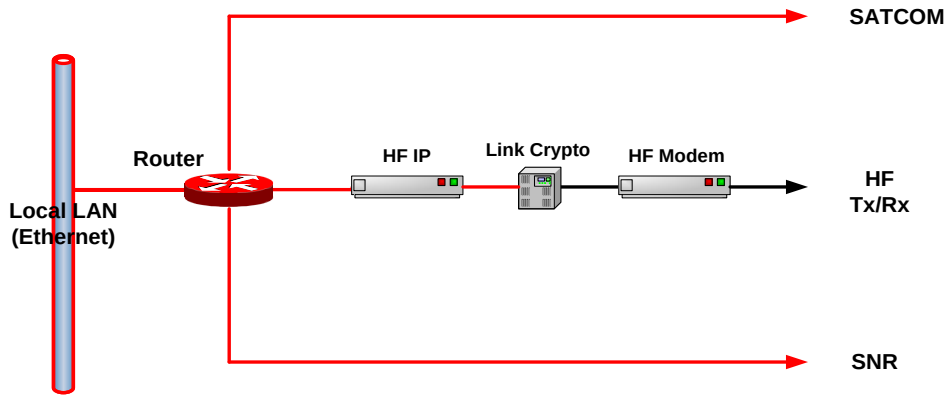

Figure 2-10 Typical Network Node Configuration

251. HF IP can be used in various network topologies. An example scenario will be that non-SATCOM ships will use HF IP to connect to a Wide Area Network (WAN) via a gateway ship that has a high bandwidth SATCOM connection to a Network Operations Center (NOC) ashore.

252. The HF IP interfaces with a COTS router that acts as the gateway for the local LAN. The router will determine whether HF or some other bearers will be used to forward IP packets, based on OSPF metrics or policy-based routing policies.

253. The HF IP is connected to the router via an Ethernet sub-net to a HF modem via a link crypto over a synchronous serial interface.

254. The HF IP supports the OSPF routing protocol and therefore can act as a default gateway for the local LAN without the use of a separate COTS router.

TECHNICAL LIMITATIONS

255. A ring can fail if one node of the ring loses two-way communications to any other members of the ring.

256. Some TCP-based applications may not work over HF IP due to its low bandwidth and high latency. When multiple bearers are available, HF IP should only be selected for forwarding IP packets of delay-tolerant applications. In order to control the IP traffic flow across multiple bearers, Quality-of-Service (QoS) or policy-based routing will have to be used.

257. The system can support multiple relays. However, current fielded capability only

functions in a three-node or greater network, so that the network latency can be kept down to an acceptable level.

BEARER ENCRYPTION ARCHITECTURES

258. Communication signals are cryptographically protected to prevent interception, disruption of reception, deception, or other exposure before they are transmitted on the air. For bearers with serial connections, type-1 military grade in-line encryptors such as KG-84A, KG-84C, KIV-7M, or KIV-7HSB are typically employed. In particular, HF IP and UHF SNR use link encryption. This equipment needs to be correctly configured and provided with appropriate key to support operations.

259. If data traffic is encrypted at the IP layer prior to transmission, then type-2 commercial grade encryption may suffice to protect transmissions on-air. This can be provided, for example, by AES-256, which is built-in to many modern modems. Various combinations of IP and link encryption may be employed to meet the requirements for communications and transmission security. In general, satellite connections are a national matter whereas direct LOS/ELOS connections require coordination between all network platforms from all participating nations.

260. The backbone of architectures, as shown in Figure 2-14, is based on non-packet-based communications systems with serial interface supporting synchronous bit streams, and is secured by Link cryptos, which provide crypto security at Layer 1 Physical, such as the KG-84 and KIV-7 family of devices. It should be noted that the word Link in Link crypto has been used to refer to synchronous or asynchronous serial links operating at the Physical layer (Layer 1) of the OSI 7-layer Reference Model.

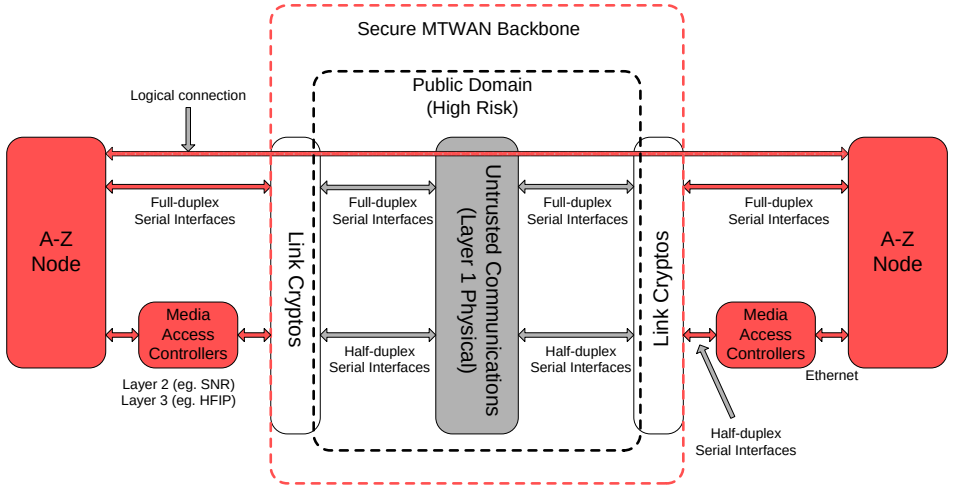

Figure 2-11 Encryption Architecture

261. Given the Link cryptos are incognizant of any data structures or communications protocols, and the secure backbone is transparent to the serial interfaces of an MTWAN node.

262. The communications systems include non-packet-based satellite services, ISDN and radio nets that support data communications over the air and over commercial telecommunications networks.

263. In addition to protecting classified information over full-duplex links such as INMARSAT B and ISDN, Link cryptos are well suited for protecting classified information over multi-member radio nets such as SNR and HFIP. This is due to the fact that Layer-1 encryption is transparent to the media access control protocols and the inherent broadcast capability of Link cryptos supports one to many connections.

264. Link cryptos typically support EIA-232, EIA-530 or military equivalent interfaces on Plain Text (PT) and also on Cypher Text (CT) for either full-duplex and simplex links. Encryption overheads are minimal and are due to the transmission of phasing and synchronisation information between two cryptos when one signals that it has data to transmit. Over a full-duplex link, the phasing and synchronisation may occur only once, as long as the cryptos remain connected. That is, there will be no encryption overheads once the phasing and synchronisation have been achieved between the two cryptos at both ends of the link. However over simplex links, such as multi-member radio nets, which provide Layer 1 (Physical) connections to SNR and HFIP, the phasing and synchronisation occur at the beginning of every transmission.

265. The architectures relying on link cryptos are known as stove-pipe where a single enclave has exclusive use of the communications links.

CHAPTER 3

ROUTING

INTRODUCTION

301. A solid network foundation is a critical requirement for effective and efficient communications in a mobile tactical network environment. In this respect routers, together with routing protocols and router configurations, are central to a strong network foundation. They enable the intelligent end-to-end movement of converged data, voice, and video information within a MTWAN and also between a MTWAN and external networks.

302. This chapter will be limited to IPv4-based networks.

AIM

303. This Chapter describes routing within a MTWAN and also between a MTWAN and external networks.

OVERVIEW

304. Routers are a network device which performs the basic function of routing IP data packets to their intended final destination or to a router which is closer to the destination. The closeness is measured by some predetermined route selection criteria such as route cost. In so doing, the routers draw upon routing protocols and algorithms to create routing tables, which the routers will use to perform the IP forwarding function. The routing protocols, such as Open Shortest Path First Version 2 (OSPFv2) and Border Gateway Protocol Version 4 (BGP4) are designed to discover and plot routes using such criteria as throughput, delay, priority and access control so that the most efficient route can be selected for each transmission. When a packet is received at a router, the router opens it, examines the network destination address, and then forwards it to its final destination or to the next router in the best route to the destination based on the information in the router's routing table.

305. Routers, under the same administrative authority, are usually grouped into an Autonomous System (AS) and run a common interior routing protocol such as OSPFv2. Routing among various AS's, with their independent interior routing protocols, are supported by exterior routing protocols such as BGP4.

306. In a MTWAN, routing is accomplished using the following standard IP protocols:

a. OSPFv2 for interior AS routing;

b. BGP4 for exterior AS routing; and

c. Protocol Independent Multicast (PIM) for multicasting.

307. Routing protocols are used by routers to exchange information on network topology and network reachability with their neighboring routers so that routing tables can be generated to support the forwarding of IP packets from their source to their final destination. As illustrated in Figure 3–1, when Router N receives a packet with a destination address A, it will consult its routing table and forward the packet to its directly connected LAN A over its interface N1. If a packet is received with a destination address B, Router N will transmit the packet out of its interface N2, as directed by its routing table, to Router M for on forwarding to LAN B. Full explanation of routing protocols is at Annex A.

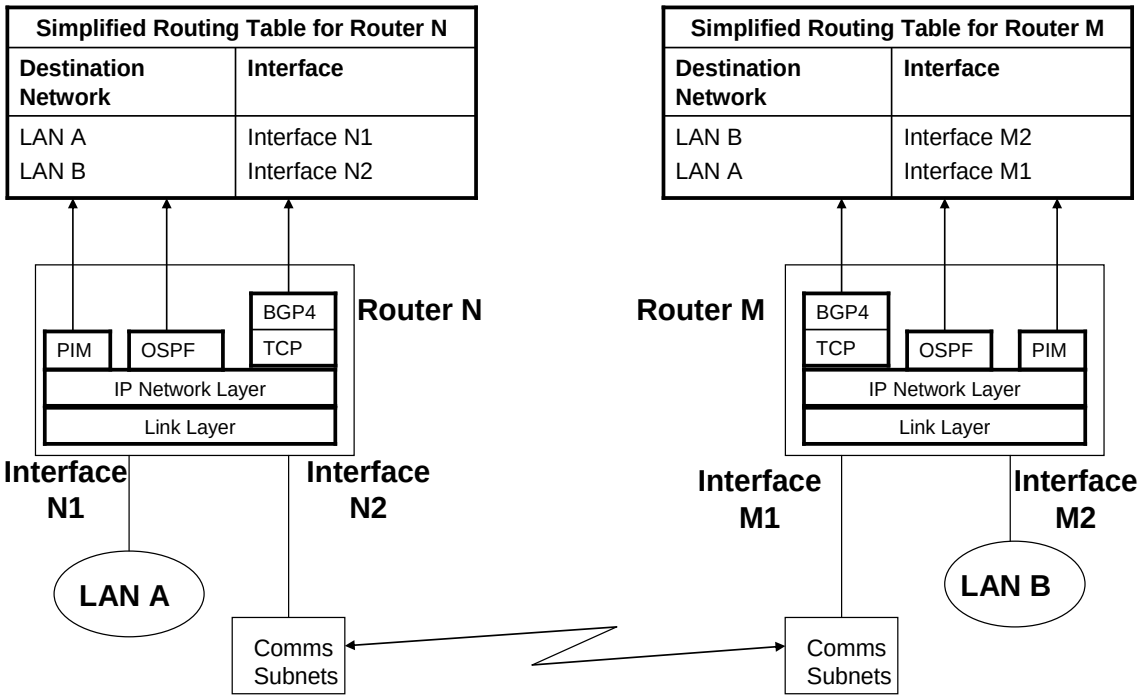

Figure 3-1 Routing

MTWAN TOPOLOGIES

308. In terms of topologies, a MTWAN either employs a single-AS topology or a multiple-AS topology. The latter is generally employed to allow nations within a MTWAN to administer their own mobile units and Network Operations Centres (NOCs).

SINGLE-AS MTWAN

309. A MTWAN of 100 nodes or less can be easily supported by a single-AS network where all mobile nodes and NOCs of the MTWAN belong to a single OSPF routing domain, as illustrated in Figure 3–2.

310. The MTWAN can be connected to other Allied WAN's of the same security classification using BGP4 with multiple BGP4 connections for redundancy.

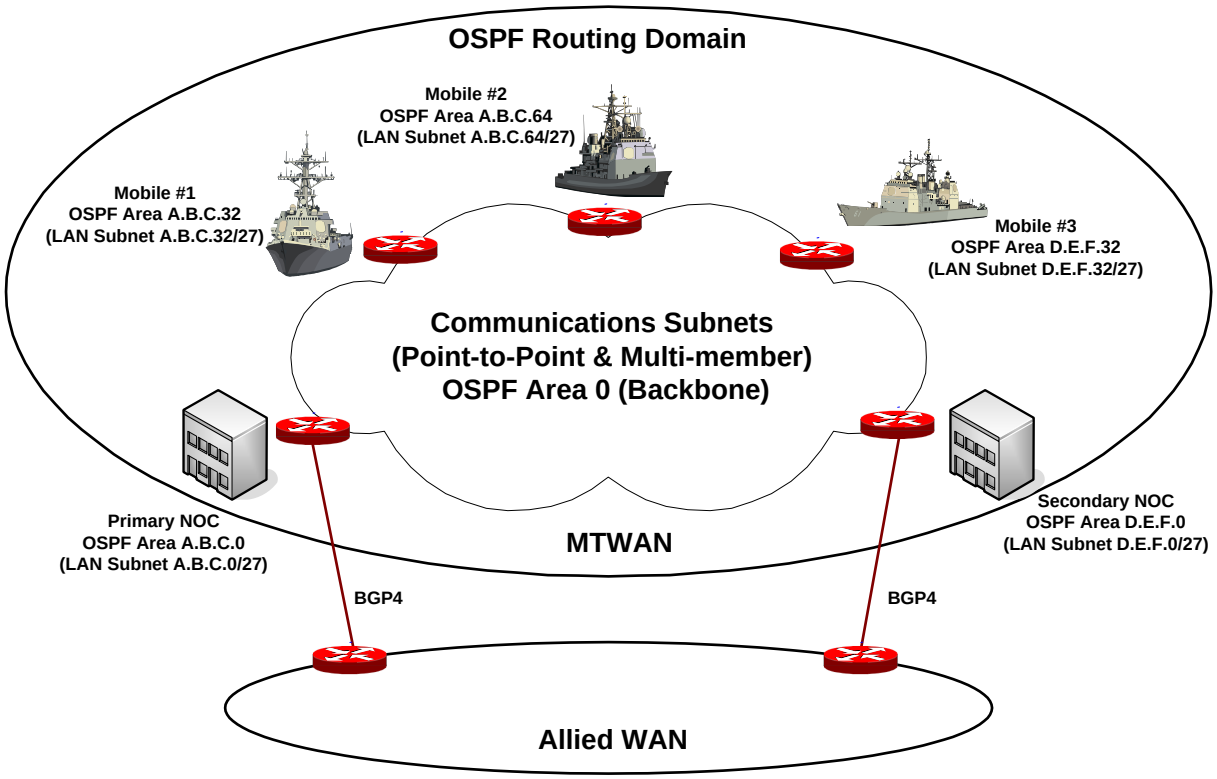

Figure 3-2 Single-AS MTWAN

MULTI-AS MTWAN

311. Each nation can form a separate AS within a MTWAN. The MTWAN is then considered as a network comprising of a number of AS's. OSPF will run internally within each AS to control path selection for all traffic flows within the AS. Connectivity between different AS's is supported by BGP4 via national NOCs as depicted in Figure 3-3.

312. As in the case for a single-AS MTWAN, a multiple-AS MTWAN can also be connected to other Allied WAN's over one or more BGP4 connections.

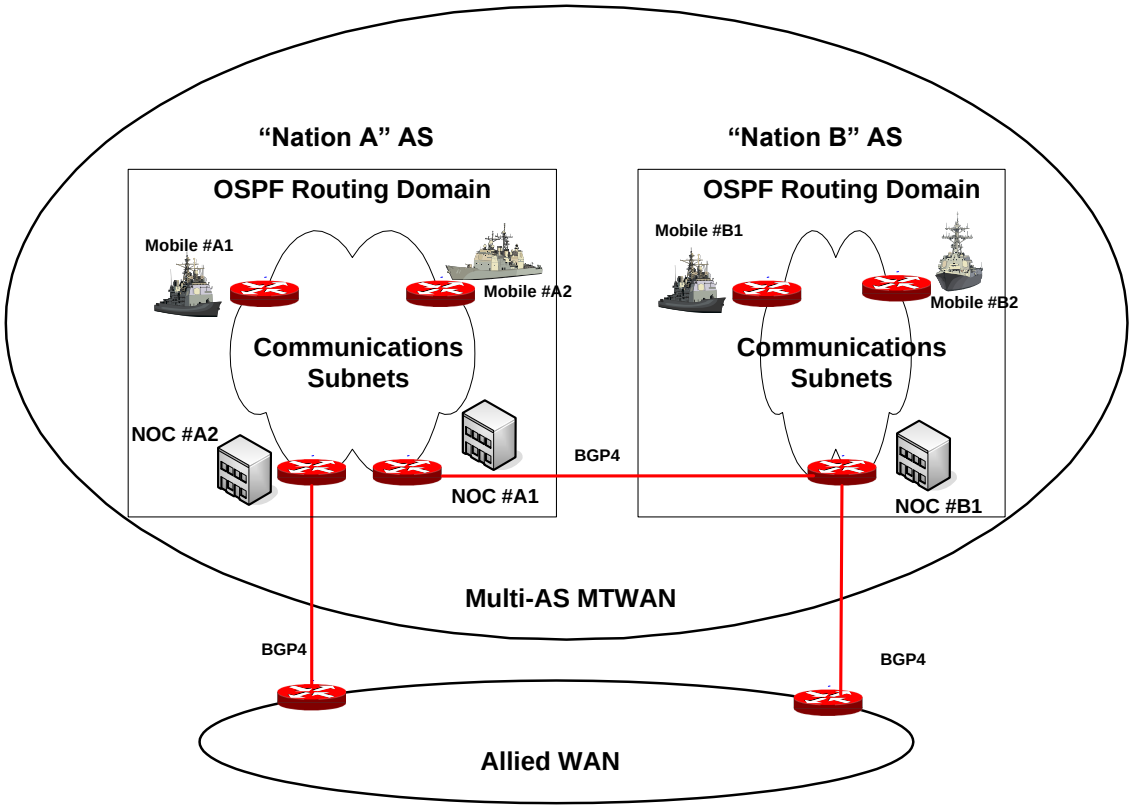

Figure 3-3 Multiple-AS MTWAN

SINGLE-AS MTWAN ROUTING

313. The MTWAN is divided into OSPF areas where all communication subnets are included in the backbone area, known as Area 0. The local area network (LAN) at each node is contained in a separate OSPF area whose number is the network address of the LAN. In the example shown in Figure 3–2, the MTWAN is allocated two Class C addresses: A.B.C.0 and D.E.F.0. The two Class C networks are divided into 16 subnets for 16 Local Area Networks (LANs) with up to 30 individual IP addresses each. Mobile #1 is assigned the network address A.B.C.32 which is also the mobile's OSPF Area Number. One or more Class C addresses are allocated for the communications subnets.

314. Communications subnets providing IP connectivity between routers over point-to-point and multi-member connections are themselves networks comprising logical and physical links. Generic Routing Encapsulation (GRE) tunnels, protected by In-line Network Encryptors (INE) over a Cipher Text (CT) Black Core or ISDN links, protected by link cryptos, are an example of point-to-point connections, and SubNet Relay (SNR) is an example of multi-member subnets. As the name suggests, the communications subnets also require IP address allocation to their interfaces with the routers and also to their own internal networks as in the case for HFIP.

315. Mobile nodes within Line Of Sight (LOS) range can communicate directly with one another via LOS networks such as SNR or HFIP. The use of LOS connectivity can significantly conserve SATCOM bandwidth by allowing direct communications between mobile nodes which are within the LOS range of each other, in lieu of two SATCOM hops via a NOC.

316. In addition to supporting direct communications between mobile nodes in a satellite denied environment, LOS connectivity can also function as a relay for traffic between a mobile node and any other node on the network during the mobile node's periods of SATCOM failure or being unavailable.

317. Direct LOS connectivity, where available, will be used for mobile-to-mobile traffic to better utilize available bandwidth.

318. Whenever possible, fixed terrestrial subnets will be selected for traffic between non-mobile units.

319. Whenever possible, the fixed terrestrial connectivity to the RF subnet of the specific mobile node that hosts the traffic endpoint will be used for fixed-to-mobile traffic.

320. Unless a mobile is acting as a relay for another mobile, its RF subnet will not be used as a transit subnet for the other mobile.

321. Route selection is to be symmetrical; traffic between two nodes should flow over the same route in both directions.

322. Within a MTWAN, route selection is governed entirely by OSPF costs, the recommended values of which can be found in Annex B. Small adjustments to the recommended OSPF metric values given in Annex B may be required so that the requirements of route selection specified above can be met.

323. OSPF uses two types of external metrics – Type 1 and Type 2 – to determine the best exit point to other routing domains or AS's. Type 1 external metrics are preferred as mobile nodes learn of several exit points, but will choose the best exit point based on OSPF costs. When the link supporting the best exit point fails, the mobile nodes will dynamically adjust their routes and select the next best exit point.

IN-LINE NETWORK ENCRYPTORS AND VIRTUAL PRIVATE NETWORKS

324. Traditional Layer-1 serial link cryptos are transparent to routing protocols. However In-line Network Encryptors (INE), also known as IP cryptos, do not support multicast OSPF updates very well; therefore Generic Routing Encapsulation (GRE) tunnels are used to support multicast and OSPF adjacencies within the MTWAN, which is protected by INEs, as shown in Figure 3.4

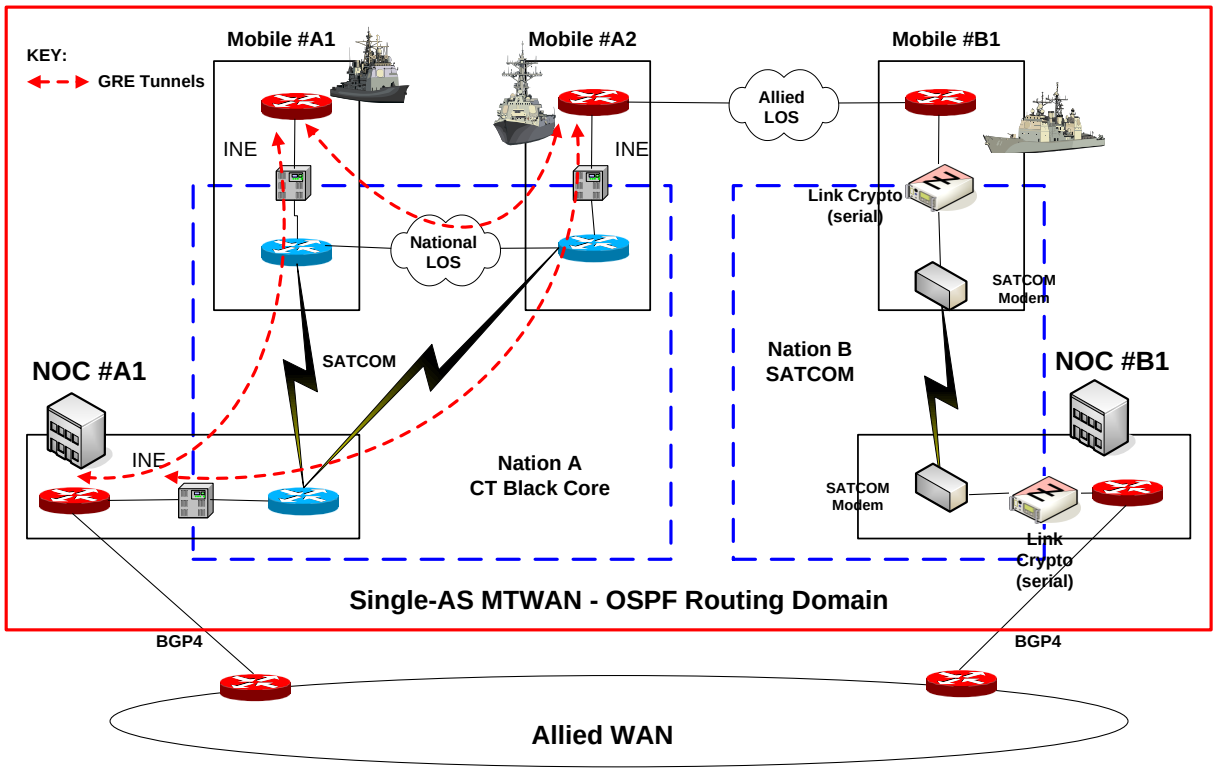

Figure 3-4 GRE Architecture

325. Connectivity between a MTWAN node and the transport backbone is via an INE. As neighbor relationships between routers of the MTWAN and the backbone do not exist, connectivity between MTWAN nodes is achieved via GRE tunnels or a routing protocol that can work through the INE.

326. The GRE tunnels can be limited to mobile-to-NOC links only. This means that any direct mobile-to-mobile traffic must go to the NOC first even if national LOS links are available. If a point-to-point GRE tunnel is set up for every national link including LOS, the number of GRE tunnels will get very large and management will be more difficult. It should also be noted that the use of GRE tunneling will also reduce the maximum transfer unit for the route because of the overhead of GRE encapsulation. As a result, the network can suffer from packet fragmentation.

327. The alternative to GRE tunneling is to use OSPF point-to-multipoint between the mobiles and the NOC as shown in Figure 3.5. This will avoid the overhead of a fully meshed network of GRE tunnels, but will allow the mobiles to announce their reachability to the NOC and, hence, inform the MTWAN of their presence. Using OSPF point-to-multipoint rather than GRE will result in a simpler and more efficient configuration when all MTWAN nodes are members of a single VPN.

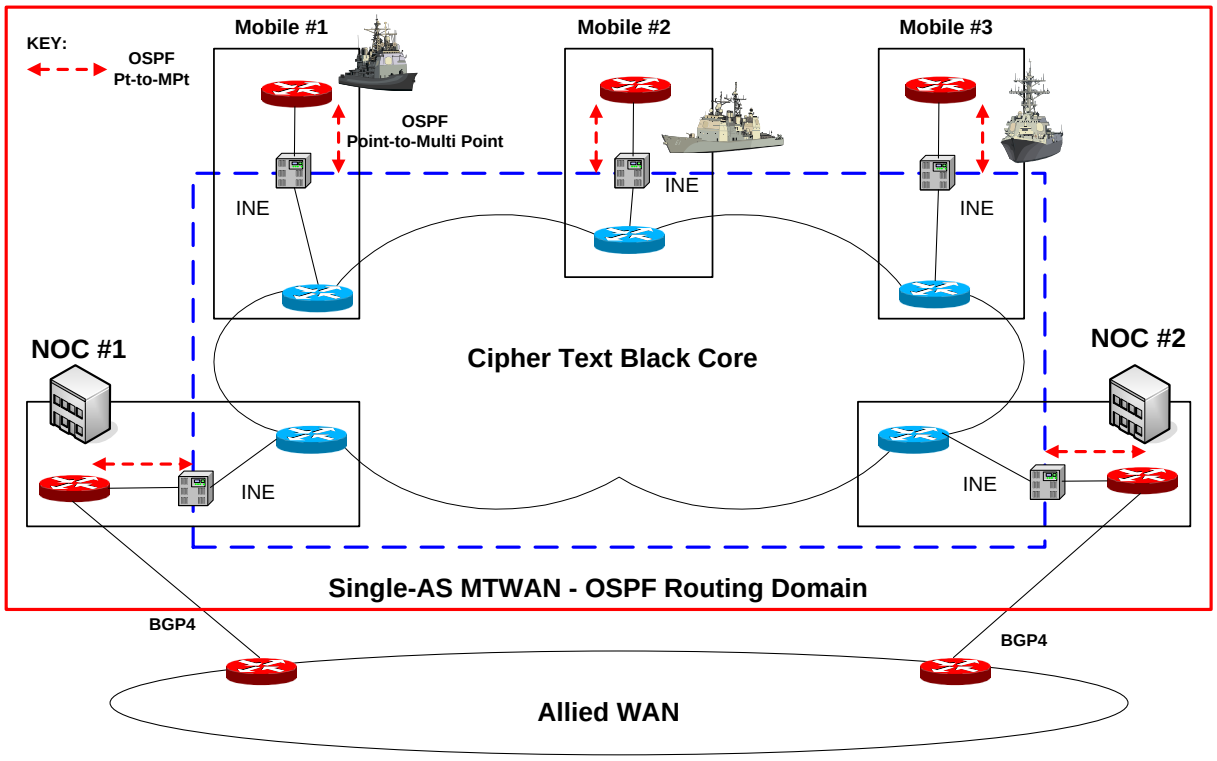

Figure 3-5 OSPF Point-to-Multi Point

MTWAN EXTERNAL CONNECTIONS

328. When connections to other networks, external to the MTWAN, exist, BGP4 is used to control which internal networks are advertised to, and which network advertisements are accepted from, other AS's. This control is at least as fine-grained as the ability to send or receive individual network advertisements. This means MTWAN network administrators have the ability to control whether to advertise or hide each individual internal network. Likewise, the administrators also have the capability to accept or reject each external network advertisement.

329. BGP4 will limit the amount of routing protocol traffic seen inside the MTWAN as a result of external links. An allied WAN has the potential to generate large amounts of routing protocol traffic. If this routing protocol traffic were allowed into the MTWAN, it might consume a significant amount of bandwidth. To prevent this, BGP4 is used to block the allied WAN routing protocol traffic into the MTWAN.

330. A global backbone network, such as the allied WAN, cannot use default routes and must have specific route advertisements for every network that is reachable across the backbone. Hence, all MTWAN nodes that are required to be visible to the allied WAN must be advertised to the allied WAN.

331. When the MTWAN has multiple connections to the allied WAN, one of the

connections will be configured to be the primary (preferred) route for all traffic between the MTWAN and allied WAN. In some cases, there may be a requirement to configure a connection to be the primary route for some nodes and the secondary (backup) route for some other nodes.

332. In order to manipulate the route selection of BGP, either of the following two BGP attributes will be used: AS-Path and Multi-Exit-Discriminator (MED).

AS-PATH

333. BGP permits BGP–enabled routers to exchange routing information with full AS-Path information. The AS-Path is a list of AS Numbers (ASNs) that describes the route between the local AS and the destination AS. When all other BGP attributes are the same, routers use the length of the AS-Path (the number of ASNs in the AS-Path) to determine the best route to a destination AS and its associated networks. A route with a shorter AS-Path is preferred.

334. A router can make the AS-Path of a route longer than the AS-Path of another route by pre-pending its own ASNs to the route's AS-Path attribute.

335. The MTWAN NOC router at the secondary site needs to be configured to pre-pend its own ASN to the AS-Path before communicating routes via BGP to the allied WAN border router. The MTWAN NOC router at the primary site does not alter the AS-Path it presents to the allied WAN.

336. For example, let 1002 be the number of the MTWAN AS. The AS-Path in routes advertised by the MTWAN NOC router at the secondary site then consist of the MTWAN ASN pre-pended to the router's AS-Path attribute, that is "1002 1002", while the AS-Path advertised by the MTWAN NOC router at the primary site simply consists of "1002". Since the AS-Path advertised at the primary site is shorter than the AS-Path advertised at the secondary site, traffic destined for the MTWAN from the allied WAN would be routed via the primary site. When the connection between the MTWAN network and the allied WAN at the primary site is not available, traffic will be re-routed via the secondary site.

337. To ensure a symmetrical path between the MTWAN and the allied WAN, allied WAN routers need to be configured in a similar fashion. The allied WAN border router at the secondary site needs to be configured to pre-pend the allied WAN ASN to the AS-Path before communicating routes via BGP to the MTWAN.

338. The primary and secondary NOC routers communicate via a BGP session to ensure a consistent view of external routing within a MTWAN AS. Using BGP, the secondary NOC router will be aware of the preferred route to the allied WAN via the primary NOC router because allied WAN routes advertised at the primary site possess a shorter AS-Path than the same routes advertised at the secondary site.

MULTI-EXIT-DISCRIMINATOR (MED)

339. MED is an alternative technique that can be used to influence route selection for traffic flowing from the allied WAN into the MTWAN. The MED feature will enable the inbound route selection to be governed entirely by the OSPF costs internal to the MTWAN. The MED effectively extends internal cost information in order to automatically control inbound route selection from the allied WAN. The BGP MED attribute is a hint to external AS's about the preferred path into an AS.

340. MED provides a dynamic way to influence routers in another external AS to choose the best route into a given AS from among multiple entry points into that AS.

341. The MED attribute only transits between a single pair of AS's, that is the receiving AS will not pass the original MED value to another AS. When the allied WAN consists of multiple AS's and the allied WAN access points are in different AS's, the BGP configuration will have to ensure that the allied WAN will make cohesive and coordinated routing decisions with respect to the preferred route to the MTWAN. This objective can be achieved by a fully meshed BGP between the AS border routers of the MTWAN and those of the allied WAN.

342. If an exit point fails, all traffic should use the remaining exit points. Failure recovery can be accomplished by setting up the default routes on the AS boundary routers. When a boundary router has a connection to the allied WAN, it needs to generate a default route and distribute it throughout the MTWAN. When a boundary router loses it's connection to the allied WAN, it needs to automatically stop generating the default route. When the failed exit point stops generating the default route, allied WAN traffic will automatically be directed to the remaining exit points by the remaining default routes.

MULTICAST

343. Multicasting within a MTWAN is supported by PIM. All COTS routers can support SM, DM and a combination of SM and DM known as Spare-Dense Mode (S-DM). When a router is configured for S-DM and a RP is not known for a group, the router will send data using DM. However, if the router discovers a RP, either dynamically or statically, SM will take over. As S-DM allows the use of both SM and DM for different groups for different applications, MTWAN routers will be configured for S-DM when multicast is required. Whenever PIM-SM is selected, a static RP at a NOC will be configured.

MULTIPLE-AS MTWAN ROUTING

344. Figure 3–6 depicts a scenario where each nation forms its own AS within the MTWAN. Within each national AS, the national backbone is used to provide connectivity between MTWAN routers using In-line Network Encryptors (INE) and GRE tunnels.

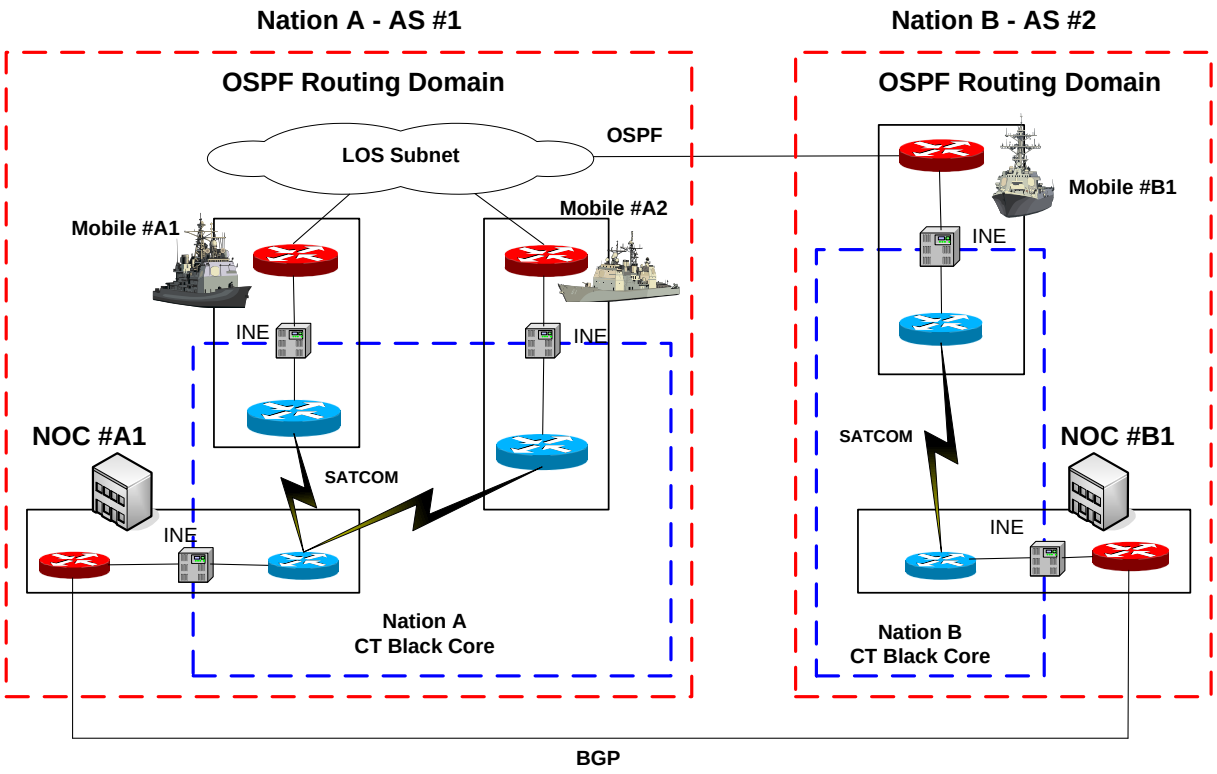

Figure 3-6 Multiple-AS MTWAN with LOS Conectivity

345. As routing over LOS subnets such as SNR and HFIP is supported by OSPF, OSPF-based LOS connectivity between nodes from different AS's, known as OSPF Backdoors, can adversely affect optimal route selection unless appropriate measures are taken on routers at the NOC's. AUSCANNZUKUS has developed a routing design that can support multiple AS's and LOS networking.

CONCLUSION

346. A MTWAN comprises one or multiple AS's, where each AS shares a common routing strategy. Internal routing is accomplished by OSPF or, in the case of multicast, PIM (SM or DM) while external routing is carried out with BGP4. The routing architecture can be complicated by multiple AS's with multiple exits and the OSPF-based LOS connectivity between mobiles belonging to different AS's. In support of the deployment of SNR and HFIP on existing multiple-AS Coalition networks, a routing design has been developed by AUSCANNZUKUS, validated in Trident Warrior for use on CENTRIXS and endorsed by M2I2. A detailed description of the design can be found at Annex C

ROUTING PROTOCOLS

ROUTING PROTOCOLS (UNICAST) – OSPF AND BGP4

1. Open Shortest Path First (OSPF). OSPF is a dynamic routing protocol that quickly finds the best route based on the lowest cost to reach the destination. OSPF assigns a metric value to each link, which is used to determine the lowest cost path from source to destination. The recommended metric values can be found in Annex A to this chapter. OSPF runs directly on top of the IP network layer. IP packets containing OSPF data will have their IP protocol number set to 89.

2. The OSPF routers exchange 5 types of Link State Advertisements (LSA's) with each other to build up the routing tables. For unicast, the IP header includes both the source and destination Class A, B, or C IP address. Each address is unique to the host computer.

3. Border Gateway Protocol Version 4 (BGP4). BGP4 is a policy-based routing protocol that selects the AS to which it will talk to based on a policy entered manually by the AS manager. It operates on top of TCP and requires very stable subnets, which are more applicable to fixed infrastructure connections.

4. BGP4 operates on top of TCP and requires two routers to set up a connection and establish a session to exchange routing information. BGP4 selects the path based on a policy that is converted into attributes. Each AS is assigned a unique AS Number (ASN) that is contained within the BGP4 protocol header. Policies then can be used to determine which AS to route traffic through or which to avoid. BGP4 does not provide the dynamic response of OSPF.

5. An AS can have more than one exit point to other AS's. When only one exit point is used, the single BGP4 border router of the AS becomes the default router for all traffic leaving the AS. However, when two or more exit points exist, routing information must be provided to OSPF to decide which BGP4 border router to select to reach the external destination. In addition, the multiple BGP4 border routers of the AS need to exchange routing information to keep their databases synchronized. This may be accomplished using the internal BGP4 protocol.

ROUTING PROTOCOLS (MULTICAST—PIM)

6. The protocol stack for Protocol Independent Multicast (PIM) is shown in Figure 3–1. PIM is directly on top of the IP network layer. IP packets containing PIM data will have their IP protocol number set to 103.

7. PIM runs over an existing unicast protocol (including static routes), and uses the information provided by the unicast protocol and the static routes to build the distribution tree

which the routers will use to forward multicast packets to all the members of the multicast group.

8. Host computers use Internet Group Management Protocol (IGMP) to announce to their local multicast routers that they wish to join a multicast group (a group D IP address). The IP header for multicast now includes a source Class A, B, or C unicast address and a destination Class D multicast group address.

9. There are two modes of operation with PIM: PIM-SM (Sparse Mode) and PIM-DM (Dense Mode).

SPARSE MODE

10. PIM-SM is designed for situations where group members are sparsely distributed across all WANs, that is, the number of nodes with group members present is significantly smaller than the total number of nodes. PIM-SM assumes that no node wants multicast data unless it is explicitly requested.

11. PIM-SM uses some selected router as a Rendezvous Point (RP), which is the root of the distribution tree where multicast senders send their IP packets by unicast. The RP then forwards the packets to all the routers that have registered with the RP.

12. The RP can be dynamic if it is announced throughout the routing domain. In that case, all other routers rely on the RP broadcast to establish the multicast tree. The RP can also be static, in which case every multicast router in the domain must be manually configured with the RP's address.

13. In a large network with few multicast receivers, PIM-SM reduces the amount of multicast traffic flooded throughout the network.

14. In a mobile environment, NOCs will be a logical choice for an RP.

DENSE MODE

15. Dense Mode. PIM-DM is designed for situations where group members are densely distributed. That is, most nodes are members of the multicast group. Multicast data is initially sent to all nodes in the network. Routers that do not have any member of the group attached to them will send a control message to remove themselves from the distribution tree.

16. PIM-DM is simpler to implement than PIM-SM as PIM-DM does not use RPs. In small networks, PIM-DM is an efficient protocol when most nodes are members of the group.

SAMPLE OSPF METRICS

1. The routing protocol OSPF is used to control path selection for all IP traffic flows within the MTWAN. Path selection is governed by OSPF link costs. Each link will be assigned a Metric Value (MV) that will be the cost used by OSPF to determine the optimum path from source to destination, which is a path with the lowest cost.

2. To encourage use of direct unit-unit LOS network connectivity, and to off-load traffic from SATCOM, SNR and HFIP metric values are lower than SATCOM. However, if the path choices are SATCOM from unit to NOC vice SATCOM-SNR-NOC (via another unit), the shortest path would be direct SATCOM unit-NOC.

Metric Value	Bandwidth (kbps)	Link
10	>10Mbps	Ship Router to LAN
30	>1 Mbps	HF IP to RF (tap0) interface
140	>1Mbps	Pier
500	32 - 2000	Subnet Relay
700	4.8 – 19.2	HFIP
900-1100	>64kbps	SATCOM/ISDN
2,220	~6.0	32 kbps UHF/5 Member
2,660	~4.8	16 kbps UHF/3 Member
Note: ‘X’ in Figures 15-B-1 and 15-B-2 signifies information that is classified.		

Table 3B1 - Recommended Metric Values

3. The algorithm used for selecting the metric value is MVn = C x MVn-1 for each halving of the bandwidth. The recommendation is C = 1.2. The metric values shown in Table 3B - 1 are based on C=1.2 rounded off to make the selection simple. The metric values are multiplied by 10 in order to increase the space between bandwidth increments for management purposes.

4. To calculate the OSPF link costs between any source and destination pair in the example, sum the metric values shown. The router will select the path with the lowest cost.

SUBNET RELAY AND HFIP ROUTING ARCHITECTURE AND PARAMETER STANDARDS FOR LOS NETWORKING ON THE MTWAN

OVERVIEW OF CURRENT SNR/HFIP ROUTING ARCHITECTURE

1. A great deal of work has been done within the Allied/Coalition communities to develop a robust routing architecture that can easily incorporate current and future Line-of-Sight (LOS) or Ship-to-Ship networks, such as Subnet Relay (SNR) and HF-IP. The configuration developed to support *ad hoc* LOS networking uses OSPF tags and BGP community strings to communicate additional routing information. It further uses specific subnets and summarizes networks to leverage the routers ability to use prefix length as a decision point for routing. Figure 3B-1, below, describe routing decisions at the major routing points needed to support *ad hoc* networking.

2. The shipboard routers mark the routes that they generate (the shipboard LAN), and those routes they receive through SNR/HFIP (or other similar LOS network), with different OSPF tags so that different routes can be distinguished accordingly at the NOC. The ship has the best visibility into which routes are locally originated, versus those it receives from SNR/HFIP, and can pass that information up to the NOC. Because the ship is the entity that joins the three networks (ship LAN, SNR/HFIP, and Shore) together it is in the best position to identify routes originating from these three networks.

3. The NOC preserves the OSPF tags passed up from the ship and passes those values up to the NOC's egress/ingress router, the OSSR. The OSSR then converts the OSPF tags into associated BGP community strings so the routes remain distinguishable. BGP AS prepend is used to add additional AS paths to routes learned from SNF/HFIP. This allows the ships' local NOC to remain the preferred path. Other NOCs serve as backup paths should an *ad hoc* (SNR/HFIP) equipped ship lose SATCOM connectivity.

4. National NOCs use route maps in BGP to assign a BGP weight of 40000 to the ship routes of other countries advertised in from their respective NOCs. This is done so that the BGP path will be preferred over the OSPF routes passed up from the ships. Adjusting the BGP weight prevents the NOC from attempting to use the SNR/HFIP route to reach *ad hoc* equipped ships while their SATCOM, with higher bandwidth, is available. A NOC will use SNR/HFIP to reach a ship only when that ship's SATCOM becomes unavailable.

5. US units will advertise their specific LAN subnet (/26) up to their local NOC while advertising a summarized route into SNR/HFIP for other NOCs to advertise out as a backup path. Out on the WAN two routes are then advertised out, the specific subnet and the summarized class C. The router treats the two, each with different subnets (/25 and

/24), as two distinct different routes and allows both to propagate into the WAN. Routers prefer the more specific route (e.g. /26 over /25, and /25 over /24). The local NOC that advertises the shorter prefix route becomes the preferred path to the ship. The NOC advertising the summarized route with the longer prefix becomes the backup path to the ship. This is important in that it automatically shifts the ship to the preferred NOC as the ship moves from one NOC to another (e.g. PRNOC to Bahrain NOC).

6. Allied and Coalition ships pass all routes (local shipboard LAN and SNR/HFIP routes) up to their NOC. The ingress/egress router at a given nation's NOC uses BGP conditional routing to advertise another nation's ship route out only if it does not see that nations ship's SATCOM tunnel subnet. When another nation's ship SATCOM tunnel subnet is advertised into BGP, national NOCs will suppress the advertisement of other nation's shipboard LAN routes associated with that tunnel subnet.

7. Within the SNR/HF-IP *ad hoc* network, OSPF link cost is used to control routing so that ship-to-ship traffic prefers SNR, HFIP, and then SATCOM. Ship-to-shore traffic prefers SATCOM, SNR, and then HFIP. Ship-to-shore traffic via SNR/HFIP is further refined so paths via ships with higher bandwidth is preferred over other ships that have lower SATCOM bandwidth.

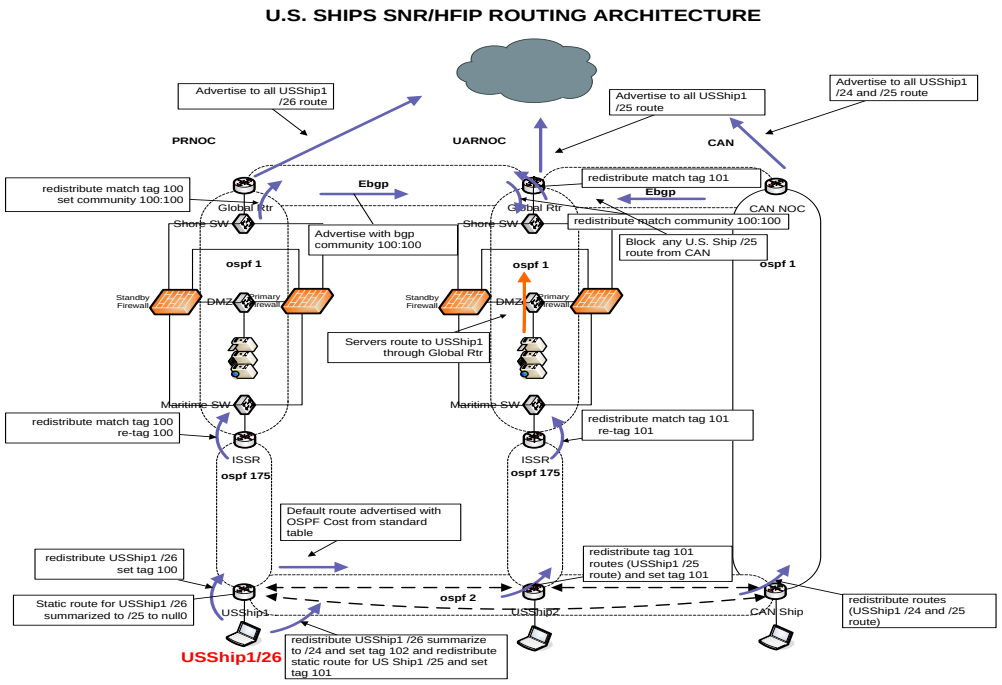

Figure 3C-1 Detailed View of US SNR/HFIP Multi-bearer Routing Configuration

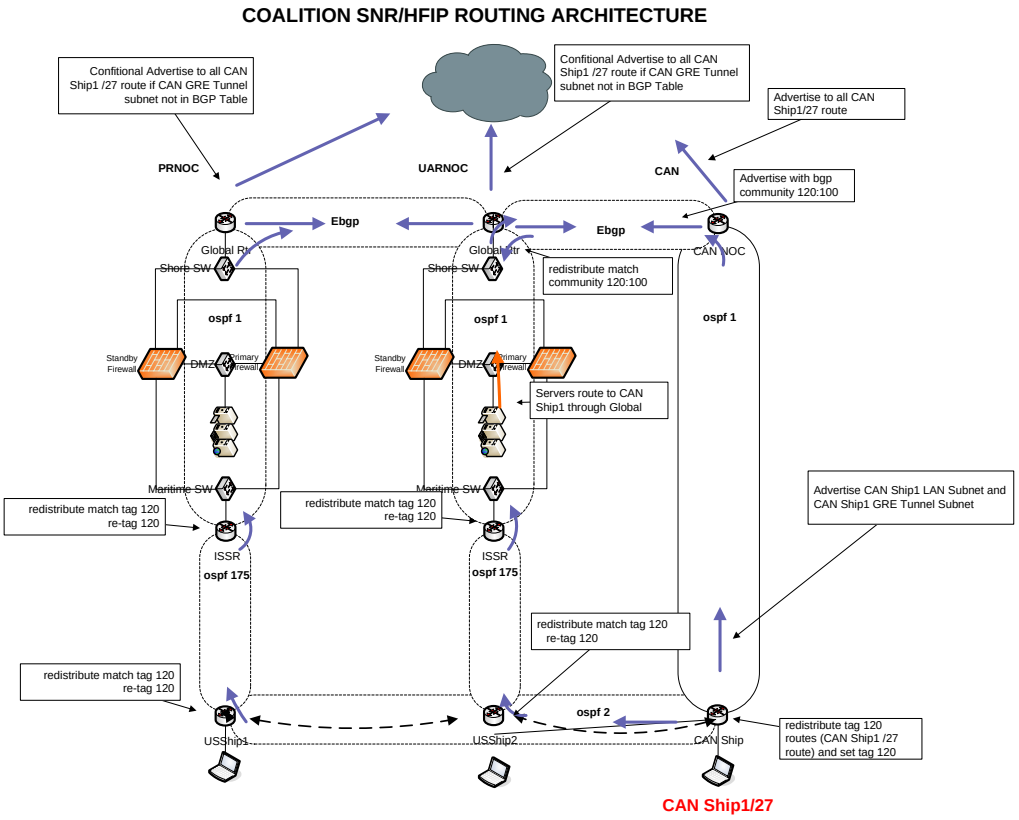

Figure 3C-2 Detailed View of Coalition SNR/HFIP Multi-bearer Routing Configuration

PARAMETER STANDARDIZATION

8. Standardization of key routing parameters for each nation is now required for an enterprise-wide solution on the MTWAN. Key parameters that must be standardized, as a function of each nation, are OSPF SATCOM Costs, OSPF LOS Networking Link Costs, OSPF Tag Numbers and BGP Community Strings.

OSPF SATCOM LINK COST STANDARDIZATION

9. Table 3C-1 is the proposed schema for assigning OSPF costs to the SATCOM link, in order to differentiate between nations. The nations listed in the table is not intended to be exhaustive, and includes those nations who have already trialled SNR and HFIP, have indicated interest in LOS networking or have a presence on various CENTRIXS enclaves.

Nation	NOC to Ship SATCOM OSPF Cost Range	Ship to NOC SATCOM OSPF Cost Range [SHIP_GRE_TUN_OSPF_COST]	Ship to Ship Default Route OSPF Cost Range [SHIP_DEF_COST]
US (GRE Tunnel for SATCOM)	900-999	900-999	790-899
US Force Level Ships	900-924	900-924	790-814
Unit Level Ships	925-999	925-999	815-899
UK	1000-1009	1000-1009	900-909
Canada	1010-1019	1010-1019	910-919
Australia	1020-1029	1020-1029	920-929
New Zealand	1030-1039	1030-1039	930-939
Netherlands	1040-1049	1040-1049	940-949
Germany	1050-1059	1050-1059	950-959
Belgium	1060-1069	1060-1069	960-969
Denmark	1070-1079	1070-1079	970-979
France	1080-1089	1080-1089	980-989
India	1090-1099	1090-1099	990-999
Italy	1100-1109	1100-1109	1000-1009
Japan	1110-1119	1110-1119	1010-1019
Norway	1120-1129	1120-1129	1020-1029
Pakistan	1130-1139	1130-1139	1030-1039
Portugal	1140-1149	1140-1149	1040-1049
Republic of Korea	1150-1159	1150-1159	1050-1059
Singapore	1160-1169	1160-1169	1060-1069
Spain	1170-1179	1170-1179	1070-1079
Other nations added as required.	Continue to increment by 10 for each new nation	Continue to increment by 10 for each new nation	Continue to increment by 10 for each new nation

Table 3C-1 Proposed SATCOM OSPF Link Cost Schema

10. Each ship should have a unique OSPF cost value whenever possible to minimize opportunities for asymmetric routing. For the U.S. Navy, the OSPF Costs used by ships in the 3rd, 5th, 7th Fleet AORs can remain constant and do not require any change as units chop from one AOR to another. The same holds true of ships in the 2nd, 4th, 6th Fleets. With the geographical separation of East and West coast platforms, there should be no physical opportunity for asymmetric routing.

11. When East and West coast platforms are in the same AOR, such as 5th Fleet, there is a slight chance for asymmetric routing to occur if ships have identical OSPS costs. The opportunities for this situation to happen are reduced, given the other routing parameters identified here. This can be ameliorated by designating all West Coast and FDNF ships to

have odd-numbered OSPF routing weights and all East Coast ships to have even-number OSPF routing weights when they are in the same AOR. An Annex specifying the routing parameters for each SNR/HFIP equipped platform can be developed and promulgated as an Annex for configuration control purposes.

LOS NETWORKING SYSTEM OSPF LINK COSTS

12. Table 3C-2 delineates the OSPF link costs that have been established for use by SNR and HFIP. HF IP OSPF costs are configured on the two interfaces that connect the Ships Coalition Router and HFIP Router together. This must be done on each interface (e.g. on the CENTRIXS router and the HFIP Router). HF IP performs OSPF routing at layer 3 with a per-hop cost of 30 over HF and 700 between the CENTRIX router and HF IP. As any future LOS networking systems become available, this table can be revisited and updated.

Link	Base Topology Link Cost	OSPF Area	Hello Interval (sec)	Re-Transmit Interval (sec)	Dead Interval (sec)
Ship Router to LAN	10				
Ship Router to SNR [SHIP_SNR_OSPF_COST]	500	1	25	40	80
Ship Router to HF IP eth0 Inteface [SHIP_HFIP_OSPF_COST]	700	1	Standard default	Standard default	Standard default
HF IP RF (tap0) interface	30	1	30	40	120

Table 3C-2 LOS Networking System OSPF Link Costs

OSPF TAG NUMBERING STANDARDIZATION

13. The OSPF Tag Numbering Schema associates specific subnets, as route summarization mechanisms, with a specific tag identifier. Table 3C-3, below, delineates these tags for seven nations for use in review and acceptance. In Schema #1, the tag numbers correlate with BGP community strings outlined in Table 3C-4. In Schema #2, the tag numbers correlate with the proposed OSPF SATCOM Link Costs outlined in Table 3C-1. Linking the OSPF Tags to the BGP Community String values outlined within this proposal is deemed an acceptable method to promote configuration management. The current OSPF tag numbers will be replaced by the proposed OSPF tag numbers. Additional nations can be provided with unique OSPF Tag Numbers as required.

Nation	Subnet	OSPF Tag Numbers
US – SATCOM	/26	100
US – Other National nodes	/25	101
US – Allied/Coalition nodes	/24	102
United Kingdom	Ships LAN	110
Canada	Ships LAN	120
Australia	Ships LAN	130
New Zealand	Ships LAN	140
Netherlands	Ships LAN	150
Germany	Ships LAN	160
Belgium	Ships LAN	170
Denmark	Ships LAN	180
France	Ships LAN	190
India	Ships LAN	200
Italy	Ships LAN	210
Japan	Ships LAN	220
Norway	Ships LAN	230
Pakistan	Ships LAN	240
Portugal	Ships LAN	250
Republic of Korea	Ships LAN	260
Singapore	Ships LAN	270
Spain	Ships LAN	280
Other nations added as required.	Ships LAN	500

Table 3C-3 OSPF Tag Numbering Schema

BGP COMMUNITY STRING STANDARDISATION

14. A unique BGP Community String is required for each national NOC. The schema developed provides a unique BGP Community String numerical identifier for each nation, followed by a 3-digit identifier that is unique to each NOC within a nation. There is sufficient room for growth within this schema. A separate Annex can be developed to track actual values for configuration control purposes.

Nation	BGP Community Strings	Example
US	100:100 – 999	PRNOC – 100:100 – 109 UARNOC – 100:120 - 129 EUNOC – 100:130 - 139 IORNOC – 100:140 – 149
UK	110:100 – 999	Northwood NOC – 110:100 – 109
Canada	120:100 – 999	Esquimalt NOC – 120:100 – 109 Halifax NOC – 120:110 – 119
Australia	130:100 – 999	Canberra NOC – 130:100 – 109 Perth NOC – 130:110 – 109
New Zealand	140:100 – 999	
Netherlands	150:100 – 999	
Germany	160:100 - 999	
Denmark	180:100 - 999	
France	190:100 - 999	
India	200:100 - 999	
Italy	210:100 - 999	
Japan	220:100 - 999	
Norway	230:100 - 999	
Pakistan	240:100 - 999	
Portugal	250:100 - 999	
Republic of Korea	260:100 - 999	
Singapore	270:100 - 999	
Spain	280:100 - 999	
Other nations added as required.		

Table 3C-4 BGP Community String Numbering Schema

SNR AND HF-IP ADDRESSING SCHEMA

15. The IP addressing Schema and standards for Subnet Relay and HF IP, developed and agreed by AUSCANNZUKUS Information Warfare and the Multi-national Maritime Information-systems Interoperability (M2I2) Steering Group are discussed in detail in the M2I2 publication: "M2I2 Ad Hoc Routing and Network Parameter Standards v2.0, February 2015."

CHAPTER 4

IP TRANSPORT SERVICES AND QUALITY OF SERVICE

INTRODUCTION

401. As a result of utilising SATCOM and other RF bearers, mobile platform communication systems are bandwidth constrained and subject to high latency and high bit error rates. These limitations can degrade application performance. Performance limitations are further aggravated by the risk of excessive packet fragmentation when cryptographic equipment and routing tunnels add headers to data packets and problems when Transport Control Protocol (TCP) is operated in the MTWAN environment. Fortunately, there are a number of strategies for avoiding and mitigating these problems in order to ensure that applications can support operational objectives.

AIM

402. The aim of this chapter is to identify reasons IP-based applications may not perform as well as expected in the Mobile Tactical Wide Area Network (MTWAN) environment and identify strategies, such as WAN Optimisation and Quality of Service (QoS) which may be implemented to improve degraded application performance caused by sub-optimal network characteristics.

MTWAN LIMITATIONS

403. The following are limitations in the MTWAN environment which impact the performance of IP applications

a. Bandwidth;

b. Latency;

c. Loss;

d. IP Fragmentation; and

e. Transport Protocol effects

BANDWIDTH

404. The principal bottlenecks for any MTWAN is the bandwidth (capacity) of its WAN links. The available bandwidth interconnecting shore-based IP routers can be very large (e.g. fibre) but on an MTWAN, the available bandwidth is very limited because of cost and technological limitations.

405. Paradoxically, simply adding bandwidth will not necessarily solve the problem of application performance on WANs. One reason is because critical applications that

suffer poor performance due to bandwidth limitations are not necessarily the applications that get access to extra capacity if it is added. Without any control to access to bandwidth, it may be less-urgent, bandwidth hungry applications that monopolize increased bandwidth.

406. LAN to WAN speed differences can be as extreme as Gb/s to Kb/s. Data gets queued at the interface to the WAN. Methods must be employed to manage this queuing of data for transmission. Unmanaged congestion at speed-conversion bottlenecks on WAN-access links can lead to unpredictable delays. TCP is the principal mechanism for controlling congestion in IP networks, but as will be discussed later in this chapter, TCP may display undesirable behaviour in an MTWAN.

LATENCY

407. Clearly network latency impacts the performance of Real Time (RT) applications such as Voice over IP (VoIP), but network latency is a critical determinant of network performance for nearly all applications in an MTWAN.

408. The round-trip time of a packet of data has a direct effect on the performance of a transactional or request/response application. High round trip times slow down "chatty" applications, even if the actual amounts of data transmitted in each transaction are not large. Since nearly all applications involve transactions as well as data transfer, delay is second in importance only to bandwidth as determinant of performance in an MTWAN. Adding bandwidth will not improve application performance when the problem is primarily latency and not bandwidth related. Once the latency exceeds the critical point for a transactional application, throughput decays quickly, regardless of the available capacity.

409. This effect is easy to understand intuitively: the rate of work that can be performed by a client-server application that executes serialized steps to accomplish its tasks is inversely proportional to the round-trip time between the client and the server. If the client-server application is bottlenecked in a serialized computation (i.e., it is "chatty"), then increasing the round-trip time by a factor of two causes the throughput to decrease by a factor of two – it takes twice as long to perform each step (while the client waits for the server and vice versa).

410. The throughput of client-server applications that are not chatty but employ window-based flow-control protocol (like TCP) to control data transfer also suffer degraded performance when latency is high. This can be understood with a simple equation that accounts for the round-trip time (RTT) and the protocol window (W). The window is how much the sender can transmit before receiving acknowledgement from the receiver. Once a window's worth of data is sent, the sender must wait until it hears from the receiver. Since it takes a round-trip time to receive the acknowledgement from the receiver, the rate at which data can be sent is simply the window size divided by the round trip time: T= W / RTT. If the window size is limited, the RTT is the limiting factor.

411. For some applications, it is not the absolute or average delay which is the primary limitation to performance, but the delay variation, e.g. the variations in delay between successive packets. Delay variation is known as jitter. Video streaming applications, for example, are relatively tolerant of delay, but are required to buffer data at the receiver in order to smooth out the delays upon playback. The size of the buffer required and the time to fill it are functions of the degree of jitter which must be accommodated.

TRANSMISSION ERRORS

412. Transmission errors result from atmospheric conditions, RF interference, congestion, incompatible configurations and limitations caused by equipment design and implementation. Acceptable Packet Loss Rate is the maximum rate at which packets can be discarded / lost during transfer through a network.

413. These causes are addressed by both error detection and error correction at all stages and by most devices in the data transmission path; but providing this protection requires additional overhead.

IP FRAGMENTATION

414. In-line Network Encryptors (INE) such as TACLANEs and VPN devices enable networks of different security classifications to share the same communications link.

415. INEs achieve this by encrypting the packet and wrapping a new packet around the outside, increasing the IP packet size. This will have an effect on the Maximum Transmission Unit (MTU) size that can be tolerated before fragmentation takes place. Fragmentation will increase network latency and therefore reduce application performance.

416. The MTU size is the maximum number of bytes that can be transmitted as a single IP packet over a network. The maximum MTU size for an Ethernet network is 1500 bytes. Any packet that exceeds this size will be fragmented into two new packets. Routers are inefficient at fragmenting and reassembling packets, this job is better done at the end points. The network will discard packets that cannot be fragmented. At the packet's final destination, the fragments of a packet will be reassembled before forwarding to the transport layer.

417. Possible solutions to the fragmentation problem include:

a. Set the MTU to a smaller value in order to allow the INE overhead to be added without taking the datagram size over 1500 bytes. One must also be cognizant of the fact that the size of the INE overhead varies depending on the encryption algorithm used. The use of routing mechanisms, such as Generic Routing Encapsulation (GRE) tunnels, will also introduce additional overheads that need to be addressed in determining appropriate

MTU size. A further consideration with the MTU size is that if it is too small, the efficiency of data throughput over the WAN will be significantly reduced.

b. Path MTU Discovery (PMTUD). The endpoint servers find the smallest MTU link in the pathway between them, and then optimise the MTU to that value.

TRANSPORT PROTOCOLS

418. IP applications such as web services, e-mail, chat, and file transfer which require reliable delivery typically use TCP for their transport layer protocol. To achieve reliable transmissions, the receiver replies with an acknowledgement (ACK) for each packet successfully received. If the ACK is not received, the sender resends the packet. TCP also implements flow control to avoid network congestion. TCP uses a sliding window to limit the amount of data that can be sent before receiving an ACK from the destination. The size W of the transmission window is dynamically adjusted by the sender in response to perceived network conditions. If packets are acknowledged, the window size is increased. If packets are not acknowledged, the window size is decreased.

419. TCP was originally developed for wired terrestrial links that have low latency and low transmission error. Packet drops were assumed to nearly always be a result of congestion at routers resulting buffer overflow. This assumption is accurate for the environment for which TCP was developed, but not necessarily for an MTWAN. As already described, SATCOM and multi-member RF nets have higher latency and higher transmission error rates which can result in frequent IP packets being dropped. When this happens, TCP will shrink the transmission window W and thus the transmission rate, perhaps inappropriately. The TCP throughput that can be achieved over a WAN link may therefore result in the available bandwidth of the link not being fully utilized.

420. IP applications which are more tolerant to loss but are concerned about minimizing delay such as voice and video typically employ User Datagram Protocol (UDP) not TCP. UDP is a minimal transport protocol. Like TCP, it provides a port number field to identify the application and a checksum to help detect errors but nothing else. UDP neither guarantees delivery nor implements congestion control.

421. Real-time protocols such as VoIP typically send application packets encapsulated in Real Time Protocol (RTP) packets which are then carried using UDP for transport. RTP provides time stamping and sequence numbering to help the receiver compensate for packet loss and jitter. RTP has a sister protocol, Real Time Control Protocol (RTCP) which the receiver uses to inform the sender about performance statistics and potentially adjust its transmission coding.

422. Another common use of UDP is to carry multicast traffic. Multicast applications are one-to-many or many-to-many. If application traffic is to be sent to multiple

recipients, it is more efficient to send it multicast that as multiple unicast, i.e. one-to-one, messages. TCP is a point-to-point protocol and so not suitable for multicast.

IMPROVING NETWORK PERFORMANCE

423. Performance enhancing techniques offer a more efficient use of limited bandwidth and adding tolerance to high latency and high bit-error rate. Any performance enhancing techniques employed must be transparent to applications. These techniques can be grouped into the following categories:

a. Multicasting;

b. Data Compression;

c. Caching;

d. Quality of Service (QoS), and

e. Performance-Enhancing Proxies

424. These techniques are discussed in the following sections.

MULTICAST GATEWAYS

425. As already mentioned, if an application sends the same data to multiple users, it may be more efficient to multicast its messages rather than send multiple unicast messages. Very few commercial IP applications including multi-party collaboration tools, however, employ the multicast paradigm. Nearly all Internet traffic is unicast. Adapting commercial applications to multicast typically involves modification of the application or the introduction of intermediate gateways to perform protocol conversion. These gateways are located on the LAN side of a router and transparently convert a TCP connection into a multicast transfer thereby removing the connection setup and management overheads of TCP. Figure 4-1 illustrates the operation of multicast routing and multicast gateways.

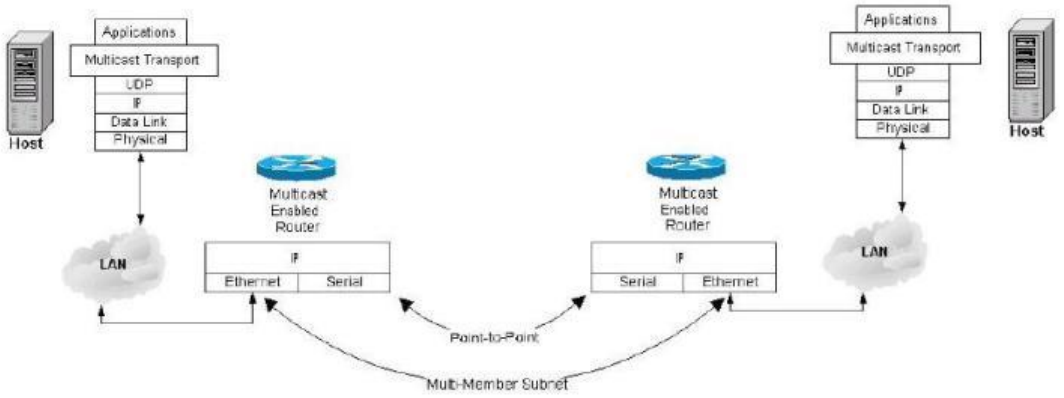

Figure 4-1 Multicasting and Multicast Gateways

426. A multicast gateway will typically send the multicast messages in UDP packets. Since UDP is, an unreliable transport protocol, the multicast gateways must implement some form of error control to guarantee successful delivery of the UDP datagrams and flow control to restrict the transmission rate so that the multicast traffic will not monopolize the WAN link. A multicast transport protocol such as Multicast Dissemination Protocol (MDP) or Negative Acknowledgement (NACK)-Oriented Multicast (NORM) can be employed on top of UDP to provide these services.

COMPRESSION

427. Compression reduces the number of bits sent by an application so that more applications can share the same WAN links. Compression algorithms are divided into two types: lossless and lossy. With lossless compression, all of the original data can be restored from the compressed version. With lossy compression, less important data is dropped in favour of the more important data. Lossy compression is executed, for example, when a jpeg image file is saved at a lower resolution. If lossy compression is performed, it is usually done by the application itself since a generic compression algorithm does not know which bits are most important and which are less so. In-line network appliances which perform compression typically employ lossless compression.

428. Compression and decompression must be implemented in pairs. Data compressed at the source must be decompressed at the destination using the same algorithms. Compression will not work efficiently on data that is already compressed (such as VoIP and streaming video). Since compression works by removing redundancy, it will not work on data that has been randomized by encryption. This includes data that is randomized by the applications (such as HTTPS and SSH) and any IP-encrypted data. For this reason, in-line compression devices must be deployed on the plain text (PT) side of network encryptors.

CACHING

429. Caching stores a copy of data, which is accessed frequently or was previously retrieved by a user over the WAN, in a cache on the user's LAN, which is particularly relevant to HTTP and Common Internet File System (CIFS) data. Commonly accessed data may also be pre-positioned prior to deployment.

QUALITY OF SERVICE

430. Quality of Service (QoS) refers to methods for providing preferential treatment to certain types of network traffic over other classes. IP only provides Best Effort Service in that traffic is processed as quickly as possible, but there is no guarantee as to timeliness or actual delivery. However, the fundamental concept behind QoS is that better service to certain traffic flows can be provided by either raising the priority of a flow or limiting the priority of another flow.

431. Quality of Service (QoS) is an encompassing term describing the collection of activities, management functions and strategies that aim at guaranteeing the end-to-end, predictable and consistent behaviour of network-dependent applications. This definition of QoS highlights the following.

432. Predictability and Consistency. A service response is predictable when the conditions for its delivery are known over a period of time. Consistency is the difference between the nature of an expected response and the actual one.

433. Guarantee. There needs to be some level of assurance in terms of predictability and consistency.

434. Management. A management function is necessary in achieving predictability and consistency and includes such mechanisms as negotiation, admission control and monitoring; and

435. Aspects of QoS are addressed at every level of the OSI 7-layer model.

436. The objective of QoS is to achieve end-to-end predictability of IP packet delivery for Command through:

a. Visibility of the WAN connection;

b. Ensuring critical application performance;

c. Controlling less urgent traffic;

d. Maximising throughput; and

e. Analysing response times, link allocation, and network efficiency.

VISIBILITY

437. Visibility of the network is a necessary first step towards implementing any QoS solution. It is important to understand what is occurring in a network (i.e. precisely which applications transverse the network, what portion of the bandwidth they consume, how well they perform, and where the delays originate, etc.) before one can effectively control and compress any traffic intelligently. Ideally, this requires a solution capable of providing in depth visibility, analysis, and trending the network.

TYPES OF APPLICATIONS

438. The application types play a major role in the network performance. Essentially there are three kinds of network applications:

a. Real-Time – Real-time (RT) applications such as Voice and Video are intolerant of delay and jitter, and typically require reserved bandwidth or priority handling. Real-time applications can be divided into elastic applications and inelastic applications. Elastic applications have the ability to adapt to variable network conditions, for example by changing the codec employed or changing the frame rate in the case of video. Inelastic applications do not adapt and therefore require the most stringent QoS.

b. Preferred – many MTWAN applications benefit from receiving special handling and being prioritized over those that are more routine, even if they are not real-time. Preferred applications include interactive applications such as text chat and mission-critical applications such as COP, messaging, and mission-critical email and web applications.

c. Routine – Routine applications include those that are most tolerant of delivery delay and those that are not mission critical. These are applications that will receive only best effort service. Examples include bulk file transfer and personal email.

439. Some architectures also distinguish a fourth class of applications that should receive a worse than best effort or least effort service. This scavenger class is reserved for applications which are not mission critical but are known as large consumers of bandwidth in networks without any QoS mechanisms. Examples of such applications might include automated file backup and some quality of life web browsing.

440. MTWAN applications / services differ widely in the QoS they require. The result of inappropriate priority and precedence can vary from information arriving late

(e.g. message delayed) to being incomprehensible (e.g. real-time video and voice with excessive latency and jitter).

CONTROLLING LESS URGENT TRAFFIC

441. Large packets delivered from lower priority, high bandwidth applications may affect the latency for higher priority, latency intolerant applications (such as voice). For example, a 1500-byte packet delivered as part of a file transfer over a 64-Kbps link will take 187 ms to be transmitted. This means a voice packet cannot be transmitted during this interval. As a result, voice cuts or delays will be heard for voice traffic queued behind this large packet.

442. Different speed links in the network may mean that packets may get queued internally in the network. When packets queue internally in the backbone of a network, latency and quality can be affected. Subsequently, it is important to regulate less urgent traffic (such as personal e-mail and internet access).

TRAFFIC CLASSIFICATION

443. To provide preferential service to a type of traffic, it must first be identified and then the packet may optionally be marked. These two tasks make up classification:

a. When the packet is identified but not marked, classification is said to be on a per-hop basis. With this per-hop basis, the classification pertains only to the device that it is on, and is not passed to the next router.

b. When packets are marked for network-wide use, the Type of Service byte in the IPv4 packet or the Traffic Class byte in the IPv6 packet can be set. Packets may also be re-marked at intermediate points in the network, but this is not recommended in general. It is better to employ a consistent marking scheme throughout.

444. Common methods of identifying flows include Access Control Lists (ACLs) and QoS profiles, policy based routing, Committed Access Rate (CAR), and Network Applications. Individual application instances (called flows) are typically identified by source and destination IP addresses, source and destination port numbers (used by TCP and UDP to identify applications), and the protocol field in the IPv4 header. The IPv6 header includes a 20-bit flow identifier field as well. Some networking appliances are able to provide additional granularity by identifying application-specific information such as email or web addresses.

CONTROL

445. Flexible policies are required to protect critical applications, to regulate bandwidth intensive traffic, to limit low priority usage, and block malicious traffic. These policies should be able to:

a. Protect the performance of important applications;

b. Contain unsanctioned and recreational traffic;

c. Provision steady streams for inelastic applications such as voice and VTC;

d. Stop applications or users from monopolizing the link;

e. Reserve or cap bandwidth; and

f. Provision bandwidth between multiple locations, groups or users.

SERVICE LEVELS

446. Service levels refer to the actual end-to-end QoS capabilities, meaning the capability of a network to deliver service needed by specific network traffic from end to end or edge to edge. The services differ in their level of QoS, which describes how tightly the service can be bound by specific bandwidth, delay, jitter, and loss characteristics.

447. Three basic levels of end-to-end QoS can be provided across a heterogeneous network, as shown in Figure 4-2:

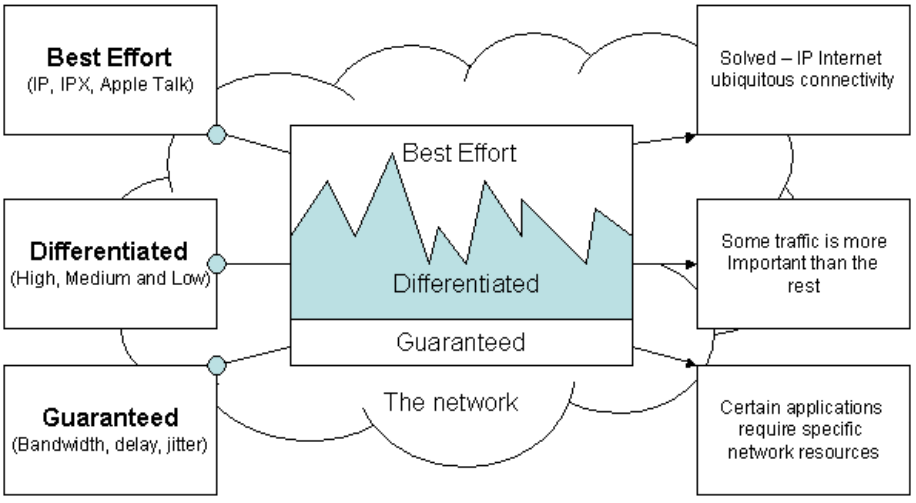

Figure 4-2 Grades of Service

448. Deciding which type of service is appropriate to deploy in the network depends upon:

a. Whether the current infrastructure can support the specific QoS methods intended;

b. The application or problem that Command is trying to solve; and

c. Whether it is simple to deploy and simple to maintain.

DIFFERENTIATED SERVICES

449. Differentiated Service (DiffServ) is a QoS architecture defined by the IETF to define and provide coarse-grained service in IP networks. The DiffServ approach defines a number of traffic classes, mandates a packet marking scheme, and specifies the particular forwarding treatment (per-hop behaviour or PHB) to be received by the packet of each class on its path from source to destination.

450. The traffic classes defined by DiffServ include an Expedited Forwarding (EF) class, a number of Assured Forwarding (AF) classes, and a Best Effort (BE) class. Expedited Forwarding is intended for traffic with very stringent delay requirements such as real-time traffic. The Assured Forwarding classes are intended for preferred traffic which needs better than best-effort treatment. There are 12 grades of Assured Forwarding defined in total. These are distinguished by forwarding priority and drop probability. Best Effort is the default class.

451. DiffServ uses the IP TOS byte for marking the class. The old TOS byte used the first 3 bits for IP precedence, the next 3 bits to indicate TOS, and the final 2 bits for explicit congestion notification (ECN). DiffServ has repurposed the first 6 bits of the TOS byte and uses these to mark packets with a Differentiated Services Code Point (DSCP). DiffServ, however, still maintains backward compatibility with IP precedence. When only the first 3 bits are employed (i.e. the next three are all zero), the resulting DSCP is called a class selector (CS).

DSCP	Decimal Value	Traffic Class	Priority/Precedence	Drop Probability
111 000	56	CS7	111(7)	
110 000	48	CS6	110(6)	
101 110	46	EF		
101 000	40	CS5	101(5) - Critical	
100 010	34	AF41		Low
100 100	36	AF42		Medium
100 110	38	AF43	100(4) - Flash	High
100 000	32	CS4	Override	
011 010	26	AF31		Low
011 100	28	AF32		Medium
011 110	30	AF33		High
011 000	24	CS3	011(3) - Flash	
010 010	18	AF21		Low
010 100	20	AF22		Medium
010 110	22	AF23		High
010 000	16	CS2	010(2) - Immediate	
001 010	10	AF11		Low
001 100	12	AF12		Medium
001 110	14	AF13		High
001 000	8	CS1	001(1) - Priority	
000 000	0	BE	000(0) - Routine	

Table 4-1 Differentiated Service Classes by DSCP

452. Table 4-1 lists the DSCP code point values and their interpretations.

PER-HOP BEHAVIOR

453. DiffServ does not proscribe precisely how traffic should be handled, but instead provides guidelines. Traffic handling is to be implemented on a per-hop basis rather than end-to-end. EF traffic should receive priority over the AF and BE classes, but may be bandwidth-limited, e.g. to 30% of the next-hop bandwidth, in order to prevent starvation of the lower priority traffic. AF traffic should be preferentially forwarded in order of priority and before BE traffic. If traffic has to be dropped, it should be dropped in order of drop probability with BE traffic dropped first. It is recommended that a mechanism such as weighted fair queuing (WFQ) be employed for the transmission of AF traffic rather than strict priority transmission in order to prevent starvation of lower-priority traffic. Like wise it is recommended that weighted random early drop (WRED) be implemented rather than strict tail drop when packets must be dropped.

454. The notation employed for the AF traffic is AF*xy* where *x* denotes the transmission priority and *y* the drop probability. This is shown in Table 4-1. Using this

notation, in the event of congestion between traffic of different priorities, AF4*y* traffic will be preferentially forwarded over AF3*y* traffic, which will in turn be forwarded before AF2*y* traffic, which will in turn be forwarded before AF1*y* traffic. If there is contention within traffic of the same priority, then traffic of class AF*x*3 will be preferred to be dropped before traffic of class AF*x*2 which will be dropped before traffic of class AF*x*1.

MAPPING APPLICATIONS TO TRAFFIC CLASSES

455. Having agreed on a selection of traffic classes and a marking scheme, MTWAN participants must also agree on which applications belong in each of the classes. A possible mapping of applications to traffic classes is provided in Table 4-2. Classes CS6 and CS7 are reserved for network control traffic. Expedited Forwarding is used for voice and sometimes for video. Real-time applications not included in EF are mapped to precedence class 4. High-priority non-real-time applications are mapped to precedence class 3. Low-latency data applications such as interactive applications are mapped to precedence class 2. After this, in precedence, class 1 appear as high-throughput mission-critical applications. Best-effort traffic and traffic that can not be identified will be marked with DSCP 0. Finally, in this table is included a least effort (LE) class for high-throughput applications that are not mission critical and other applications for which a less than best effort service is desired. The choice of DSCP marking for this so-called scavenger class is not standardized. In this table, the DSCP for CS1 has been selected for scavenger class.

Application or Traffic Type	DSCP	Traffic Class
Routing and network control	48	CS6
Precedence Group 5 - voice		
Voice	46	EF
Precedence Group 4 - other real time apps		
Video	38	AF43
Precedence Group 3 - high priority data		
Fires Support	26	AF31
Chat	28	AF32
COP	30	AF33
Precedence Group 2 - low-latency data		
Interactive apps	18	AF21
Directory services	20	AF22
Mission-critical web	22	AF23
Precedence Group 1 - high-throughput mission-critical		
Email, messaging	10	AF11
File transfer	12	AF12
Database replication	14	AF13
Precedence Group 0 - Best Effort		
Recreational email, default traffic	0	BE
Least Effort		
Recreational web, file backup	8	CS1

Table 4-2 Example of QoS packet markings for a MTWAN

IMPLICATIONS OF IP CRYTPO

456. In order to implement QoS throughout the network, it is necessary to have visibility of the packet markings in the network core. During IP encryption, the IP packet is encrypted and encapsulated in another IP packet with a new IP header. The original TOS byte will be encrypted along with the original packet. To provide QoS in the core, it is essential that the IP crypto copy the TOS byte into the new header. To prevent traffic analysis, it may in some cases be necessary that some of the TOS bits are copied, effectively aggregating traffic classes, or they are cleared entirely, so that delivery reverts to best effort.

TRANSPORT AND APPLICATION ENHANCING PROXIES

457. One way to mitigate the limitations of standard TCP over low-bandwidth, high-delay, and lossy connections such as those that are present in an MTWAN is to replace it with a transport protocol that is better suited for the environment. A standard TCP implementation is TCP Reno with cumulative ACK. An alternative is to use TCP Vegas

with a selective ACK. TCP Reno uses packet loss to signal congestion control whereas TCP Vegas uses packet delay. With a cumulative ACK, once a packet has been reported lost, that packet and all subsequent packets are retransmitted at the receiver. With a selective ACK (SACK), only the packets reported lost are retransmitted. It should be emphasized that TCP Vegas with SACK is by no means the only alternative to standard TCP available. This is only meant as an illustration.

458. Unfortunately, it is not in general practical to replace the TCP stack running on all hosts and servers in the network with an alternative. A TCP proxy can be inserted between the local networks and the wide area RF links. The proxy terminates the connections locally then runs a transport protocol optimized for the wide area network over the segments which need it and reconstructs the connection using standard TCP at the other end.

459. Similar proxies can be run not only for TCP but for the applications which rely on TCP and UDP for transport. An application proxy can accelerate data transfer by removing redundant data from transactions when bandwidth is constrained or parallelizing transactions which are normally implemented serially to reduce the time to complete them when the network has high delays. These proxies must of course operate on the Plaint Text (PT) side of the IP cryptos in the architecture.

WAN OPTIMIZERS

460. WAN Optimizers are multi-function devices that can incorporate several performance enhancement techniques, including data compression, caching, TCP acceleration and acceleration of select applications. In addition to optimisation, WAN Optimisers offer Traffic Marking and Shaping (QoS policy enforcement). WAN Optimisers can also provide network monitoring functions.

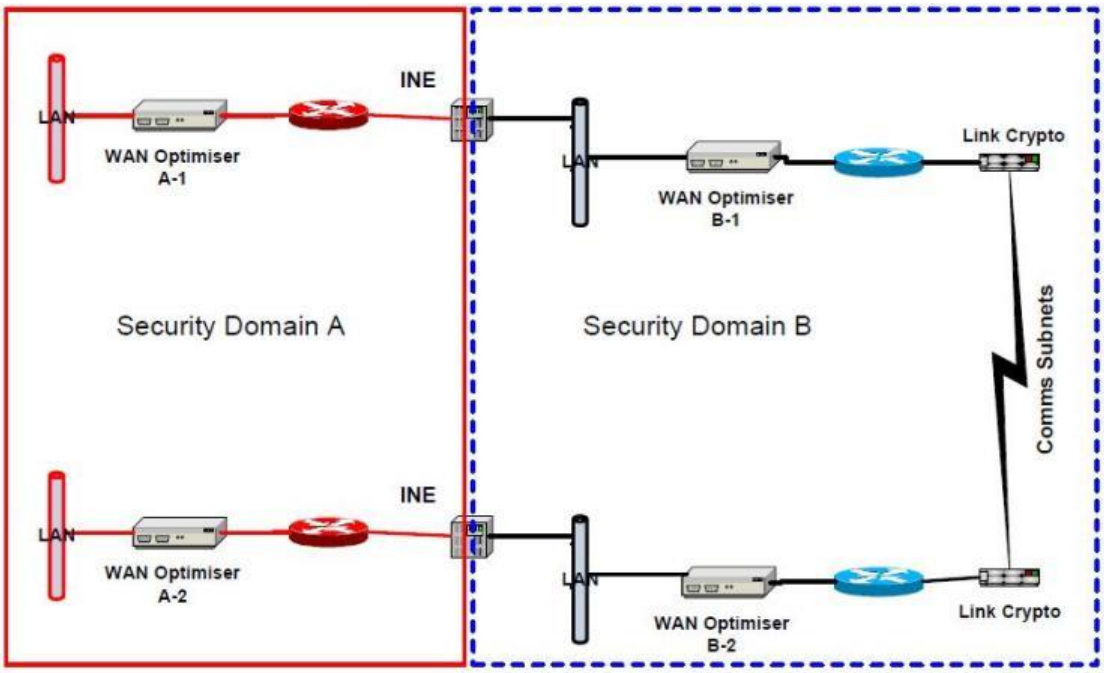

Figure 4-3 WAN Optimizers

461. Figure 4-3 shows a typical deployment of WAN Optimizers in an MTWAN where IP traffic of one security domain is tunnelled through a network of a different security domain using INEs. WAN Optimizers A-1 and A-2 can be used to compress, cache, monitor, and shape traffic from Security Domain A.

462. As IP traffic from Security Domain A will be encrypted by the INEs before it arrives at WAN Optimizers B-1 and B- 2, these optimizers will not be able to compress it, or exercise control over individual applications or TCP connections of the Security Domain A.

463. In a typical MTWAN deployment, WAN optimisers are used to mark the packets for QoS (via DSCP marking) and QoS is usually applied at the router that connects to the bearer. This is so that mission critical traffic from all network classifications can be sent over the link according to its priority.

464. Network monitoring enables performance metrics to be gathered to ensure that the link is being used efficiently and to identify the applications that are using how much bandwidth and when. It is also useful as a troubleshooting tool.

465. Application and network optimisation requires at least two WAN optimisation devices, one deployed at each end of a connection. Each device optimises its outbound traffic using various optimisation techniques, and each unit at the receiving end will restore the traffic to its original state.

466. Presently, the feature sets and technologies used are vendor specific and are not interoperable with each other. The best use of Optimizers is currently on national links until a vendor/device is agreed by multi-nations for interoperable links.

CHAPTER 5

SECURITY

INTRODUCTION

501. To support secure operations, an MTWAN requires the application of appropriate security controls. Security controls are safeguards and countermeasures employed within the MTWAN to protect the confidentiality, integrity, and availability of the network and the information it carries. There are two distinct components of security: the security architecture and the plan for its implementation versus its actual implementation and its day-to-day operation

502. This chapter establishes the technical security standards for MTWAN networks, instantiations, and interconnected component systems. The use of these guidelines is recommended to assure that the appropriate technical security controls are implemented for secure and available operation of mission critical systems. This document will further define the conceptual threats and recommended protection mechanisms to establish confidentiality, integrity and availability of MTWAN networks.

AIM

503. This chapter addresses the technical aspects of the MTWAN security architecture and recommendations for implementing protection mechanisms to protect, monitor, analyze and detect, and respond to security threats.

504. The threats section identifies technical security threats that could potentially pose risk to the MTWAN network. The protection mechanisms section identifies and defines technical measures that may be employed to mitigate the risks from potential network threats. The MTWAN security models section will provide the recommended protection mechanisms to mitigate potential threats mapped to the instantiations of security architectures. Annex A to this chapter provides security architecture and design considerations in more detail.

THREATS

505. This section identifies potential threats and vulnerabilities of MTWAN networks from a technical perspective. This includes the categorization of threat areas presented in a threat taxonomy according to the three tenets of security; confidentiality, integrity, and availability.

506. A threat is something that can go wrong. A full risk assessment considers the likelihood that a threat will be exploited and the impact to mission capability if it is. Therefore, a risk assessment in a given scenario requires knowledge of the mission objectives and knowledge or assumptions about the capabilities of potential adversaries. Such assessments are typically classified. The discussion here is conceptual only and is not a replacement for detailed analysis. Whenever possible, a full risk assessment should

be conducted by the nations in a coalition, either separately or collaboratively, prior to conducting operations.

THREATH IDENTIFICATION AND CATEGORISATION

507. Utilizing the threats as catalogued in the International Organization for Standardization ISO/IEC 27033-3:2010(E) Annex B, the following is a listing of the three major categorized threats.

a. Threats to confidentiality;

b. Threats to integrity; and

c. Threats to availability.

THREATS TO CONFIDENTIALITY

508. The loss of confidentiality of information on MTWAN networks refers to the disclosure of information to unauthorized individuals or systems. Examples of threats to confidentiality are:

a. Misrepresenting authority and rights;

b. Theft of service;

c. Invasion of privacy and eavesdropping;

d. Unauthorized network scans and probes;

e. Theft of content; and

f. Access to inappropriate content.

THREATS TO INTEGRITY

509. The loss of Integrity of information on MTWAN networks refers to the system's ability to maintain and assure the accuracy and consistency of data over its entire life-cycle. This means that data cannot be modified in an unauthorized or undetected manner. Examples of threats to integrity are:

a. Interception and modification;

b. Malformed packets and messages;

c. Compromise of installed software, service-related data, or system configuration;

d. Compromise of application data;

e. Compromise of user information; and

f. Unauthorized management.

THREATS TO AVAILABILITY

510. The loss of availability of information on MTWAN networks refers to the system's ability to assure that information and data is available when needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Ensuring availability also involves preventing denial-of-service (DoS) attacks such as:

a. Traffic/packet flooding;

b. Spoofed messages;

c. Underlying platform DoS;

d. Resource exhaustion; and

e. Session hijacking and service masquerading.

PROTECTION MECHANISMS

511. In order to ensure the addressing of all potential threat areas of MTWAN networks it is necessary to identify potential network and system protection mechanisms. These protection mechanisms will serve as mitigating controls for when a threat becomes a risk. Table 5-1 provides an overview of possible protection mechanisms for addressing threats.

Protection Mechanism	Definition
Authentication	Involves the validation of identification credentials for system users and system services.
Access Control	Involves managing access to and modification of system data and resources.

Protection Mechanism	Definition
Monitoring and Management	Involves aggregating updates from critical system resources to a comprehensive view of the network presented at a central location. Monitoring allows for rapid fault isolation and initiation of troubleshooting procedures to resolve availability issues.
Logging	Involves defining and capturing significant network events. Through review of significant events administrative staff is able to identify anomalous behavior and potentially subvert future attacks. Logging is typically an embedded function of an application or group of applications.
Backup and Recovery	Involves duplication and redundant storage of critical system data through automated procedures. Backup and recovery also involves the automated procedures to restore critical system data in the event of a disaster or traumatic network event.
Encryption	Involves the protection of system data through cryptographic algorithms and keys. Random keys are shared between communication partners and used to seed cryptographic algorithms.
Traffic Screening	Involves managing data flow to ensure that communication sessions are authorized before traversing or connecting to a specific network or network node. Traffic screening occurs primarily at OSI Layer 3, the network layer.
Packet Inspection	Involves de-encapsulation and analysis of data flow including and above OSI Layer 3. Packet inspection offers more advanced protection and is capable of detecting and protecting against network penetration attempts.
Anti-Malware	Involves automated processes, such as scanning, to identify, quarantine, and remove malicious software programs.
Patch Management	Involves automated scanning, distribution, and application of software and firmware updates to system resources.

Table 5-1: Protection Mechanisms

512. These protection mechanisms can be deployed at various and multiple points in the network architecture. Figure 5-1 depicts a notional MTWAN with three protection zones: the wide area network (WAN), the local area network (LAN), and the end user devices. Table 5-2 indicates in which zone each of the protection mechanisms of Table 5-1 can be effectively deployed. Each mechanism has also been mapped to the primary attribute it is designed to protect: Confidentiality (C), Integrity (I), or Availability (A). This does not preclude a mechanism protecting multiple attributes.

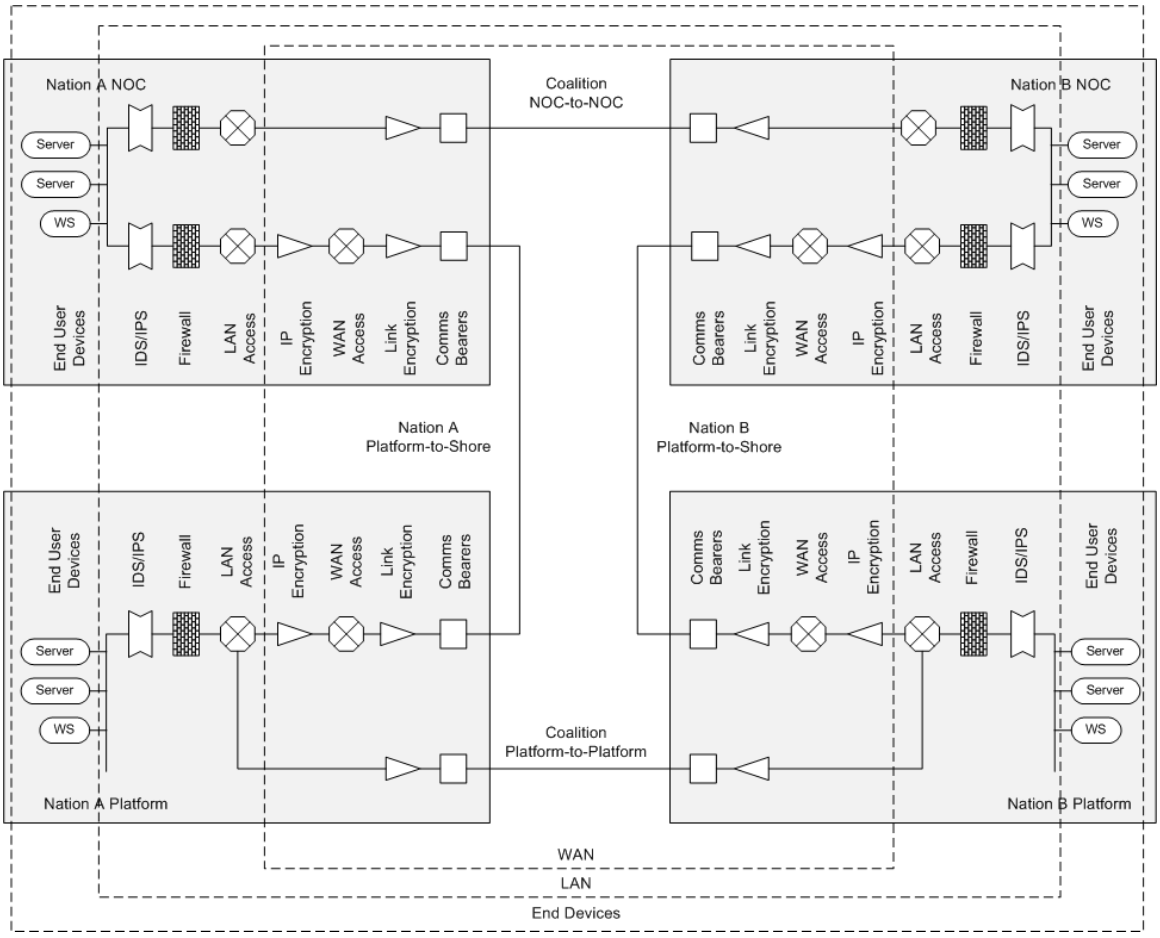

Figure 5-1: Network Architecture with Security Zones

Protection Mechanism	WAN	LAN	Device	Attribute
Access Control	✓	✓	✓	I
Anti-Malware		✓	✓	I
Authentication	✓	✓	✓	I
Backup and Recovery	✓	✓	✓	A
Configuration Management			✓	I
Encryption of Data at Rest			✓	C
Encryption of Data in Transit	✓			C
Intrusion Detection	✓	✓	✓	C
Logging	✓	✓	✓	A
Monitoring	✓	✓	✓	A
Patch Management			✓	I
Traffic Screening		✓		C

Table 5-2: Deployment Zone and Attribute Protected

513. All three zones can and should implement authentication and access control to insure the integrity of the system and some level of monitoring, management, backup, and recovery to help insure system availability. Confidentiality of data in transit is insured by encryption – one of the main functions of the WAN. All data on the air must be bulk encrypted. IP data is typically IP encrypted prior to bulk encryption to provide additional Communication Security (COMSEC).

514. Because the user data on the WAN is encrypted, it is not possible to perform deep packet inspection there. Traffic screen, packet inspection, and in-line malware scanning are executed at the LAN after decryption and before data is passed to the end user devices.

515. Malware detection and protection, i.e. anti-virus, can and should also be run on end user devices. An additional important security mechanism available to end devices is automated patch management. There can be a wide range of software running on servers and workstations and software patches to repair vulnerabilities are frequently released. Automating their installation can provide an operational advantage.

MTWAN SECURITY MODELS

516. Implementation of protection mechanisms, even all the mechanisms discussed in the previous section, will not insure that the MTWAN is secure. No system is 100% secure. What is needed is enough protection so that the residual risk remaining after their application is acceptable. This section offers general guidance on the implementation of protection measures on a MTWAN. Annex A to this chapter provides more detail on this topic. Note that, in the face of operational exigencies, deviation from these recommendations is to be expected.

517. It is not feasible to expect the full suite of protection measures to be implemented at every platform and facility. MTWAN nodes can be classified according to their ability to detect, defend, and respond to security threats. Small platforms with limited connectivity, e.g. ships with a fly-away kit which connect only to a NOC over SATCOM, can inherit security protections from their points of connection. Such a node may be adequately served by a minimal set of protection mechanisms. A better-equipped node with more diverse connectivity, e.g. a ship with LOS as well as SATCOM connections, is expected to offer protections beyond the bare minimum. The largest nodes, e.g. a big decks and for certain a NOC, is expected to offer a full suite of security protections.

518. Table 5-3 provides recommendations for protection mechanisms to be implemented at nodes of different capabilities: small, medium, and large. The small node recommendations are the minimum set of mechanisms needed for even the most disadvantaged MTWAN platforms. The large node recommendations are the Gold standard and include all of the measures listed in Table 5-1. At the minimum, these should be implanted at all national NOCs.

Node	Recommended Protection Mechanisms
Small Node	Host-based malware detection and prevention Host-based intrusion detection Automatic authentication and access control Recovery procedures Encryption of data in transit
Medium Node	Host-based malware detection and prevention Host-based intrusion detection Automatic authentication and access control Automatic Recovery mechanisms Network monitoring and event logging Packet inspection, e.g. with a Firewall appliance Encryption of data in transit
Large Node	Host-based malware detection and prevention Host-based intrusion detection Automatic authentication and access control Automatic Backup and Recovery Automated software patch management Network monitoring and event logging Network management tools Packet inspection, e.g. with a Firewall appliance Network-based intrusion detection and prevention In-line malware detection Encryption of data in transit

Table 5-3: Protection Mechanisms by Node Size

SECURITY ARCHITECTURE AND DESIGN CONSIDERATIONS

1. Information security (INFOSEC) is the protection of information systems against unauthorized access to, or modification of, information, whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. INFOSEC is achieved through a combination of the following aspects of security:

a. Personnel security;

b. Physical security;

c. Emanation security (EMSEC), also known as TEMPEST;

d. Transmission security (TRANSEC);

e. Crypto security; and

f. Computer security.

2. Technical security architectures are system-level sets of technical security measures selected and organized in a logical and effective manner to protect the confidentiality, integrity, and availability of Coalition information at a level determined through risk assessment and accepted by the information owner, and approved by national Security Authorities.

3. The MTWAN will be operating in the System-High mode, and must be capable of supporting the exchange of information classified up to Secret releasable to AUSCANNZUKUS (A-Z) nations.

REFERENCES

4. The principal security reference for any MTWAN is ACP 122. In terms of security policies and procedures this publication is subordinate to ACP 122. Where / if any discrepancies occur, doctrine within ACP 122 should be followed. The AUSCANNZUKUS Coalition High Assurance Internet Protocol Encryptor Interoperability Standard (HAIPE) profile is the primary publication for the setting up and use of HAIPE.

COMPUTER NETWORK DEFENCE (CND)

5. Network availability is supported by the use of multiple communications links to enable multiple routes to a destination. Denial of Service (DoS) attacks can occur within the Cypher Text (CT) core by various means such as disrupting radio transmissions or

flooding the commercial IP networks which support the CT core. DoS attacks can also occur on the LAN by saturating a service with requests to make the service unavailable to users. Defence against DoS is difficult. However, the risk of the MTWAN being disrupted or degraded can be greatly reduced by implementing a number of DoS mitigation designs, such as communications redundancy, Quality of Service (QoS), firewalls and computer security.

6. Protection of local network and application services against remote threats may require the installation of a firewall on the LANs. In conjunction with national Security Authority and other nation members of the MTWAN, a Threat Assessment needs to be conducted to identify the requirements for and configuration settings of the firewall. The firewall may provide some or all of the following functions:

a. Packet-level filtering;

b. Address translation;

c. Port number filtering; and

d. Application proxying.

7. Servers and user workstations must be provided with, as the minimum, anti-virus software, patching systems for applications and operating systems, application whitelisting and tightly controlled administrator privileges. Patching the operating systems and applications is to remove their security vulnerabilities. The implementation of an Application Whitelisting system will ensure that malicious software will be prevented from running on the network. Controlling and restricting administrator privileges will prevent unauthorised access to user and system information, and malicious software from spreading or hiding on the LANs.

CIPHER TEXT CORE

8. Cipher Text (CT) core is an IP-based transport network that enables enclaves of different security levels to share a common communications infrastructure supported by wired and wireless links, using Virtual Private Network (VPN) technologies, as shown in Figure 5A-1.

9. CT core architectures enabled by the introduction of Type 1 Layer-3 encryptors, also known as IP cryptos, allow enclaves of various security classifications to share communications links and therefore make better use of the available bandwidth. There are times when some enclaves have no traffic to transmit and these quiet periods can be used by other enclaves. IP cryptos are used to create secure IP tunnels between the nodes of an enclave over a shared transport network. This is the basis of Virtual Private Networks (VPN). IP cryptos typically support Ethernet interfaces on both PT and CT.

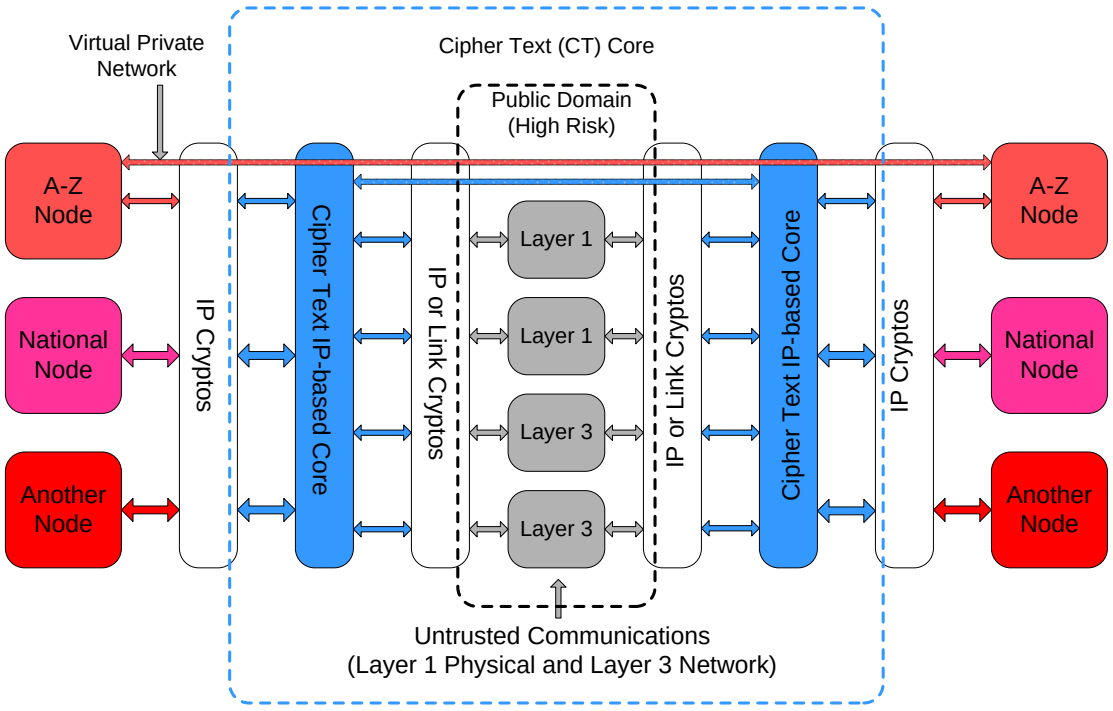

Figure 5A-1 Cipher Text (CT) Core Architecture

10. A standard for IP cryptos, known as HAIPE has been developed by the US and adopted for use by the A-Z.

11. National CT Core has been implemented by a number of nations to provide IP connectivity for Coalition and national traffic among national nodes. The core will only carry national and Coalition traffic. The security classification of the information processed by each enclave will dictate the level of protection for that enclave. As illustrated in Figure 5A-2, VPNs that connect highly classified enclaves of MTWAN and "National 1" are protected by HAIPE devices, whilst Type 2 IPSec provided by commercial IP routers and VPN devices is sufficient to protect other enclaves. Only commercial crypto security devices, which have been accredited by the national Security Authority, can be used. In addition, the configurations of IPSec and VPN must be subjected to approval from the national Certification and Accreditation Authority.

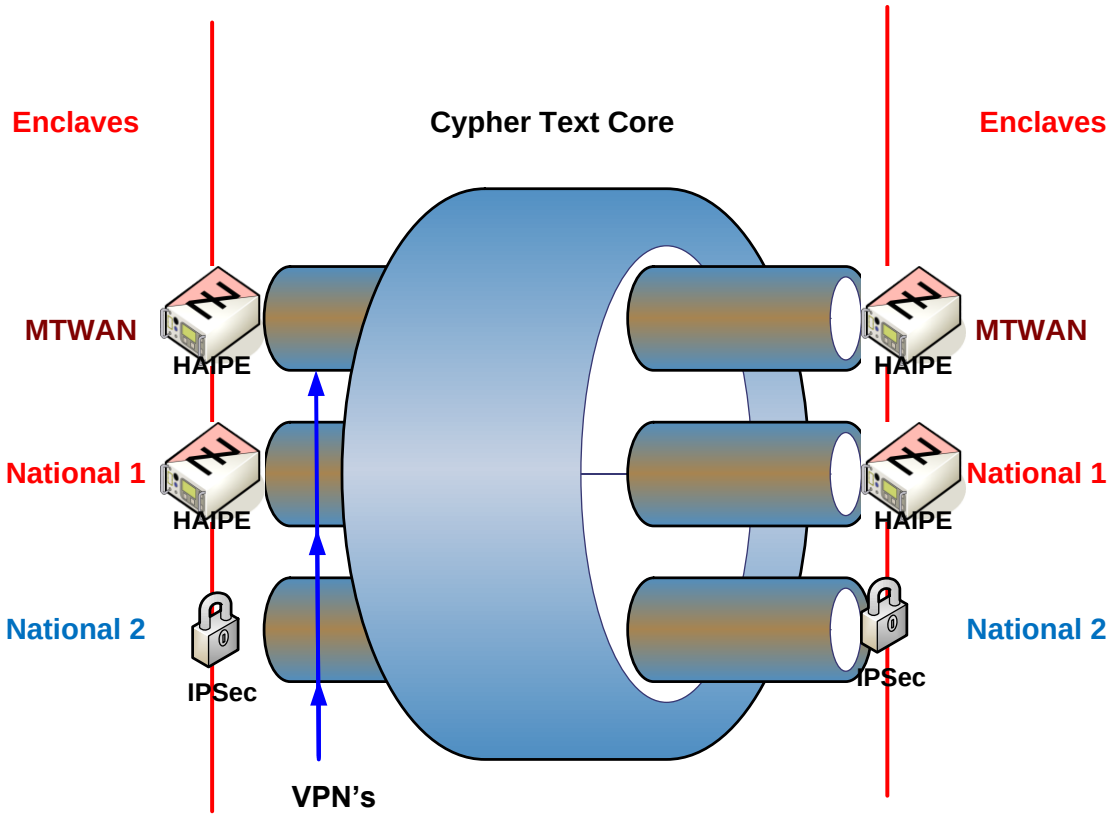

Figure 5A-2 National CT Core Virtual Private Networks

12. A typical ship node based on the national CT Core architecture is shown in Figure 5A-3. Also shown in Figures 5A-4 and 5A-5, the CT core is connected to the untrusted communications links via another layer of crypto security. Even though IP traffic from the classified enclaves is secured by the IP cryptos or IPSec, Traffic Analysis can still be performed on the core that transport encrypted traffic from all national and Coalition enclaves. Information of value may also be derived from intercept and analysis of IP headers from the CT interface of the cryptos. Therefore, some level of protection for the core will be required. The level of protection will normally be dictated by national Security policies.

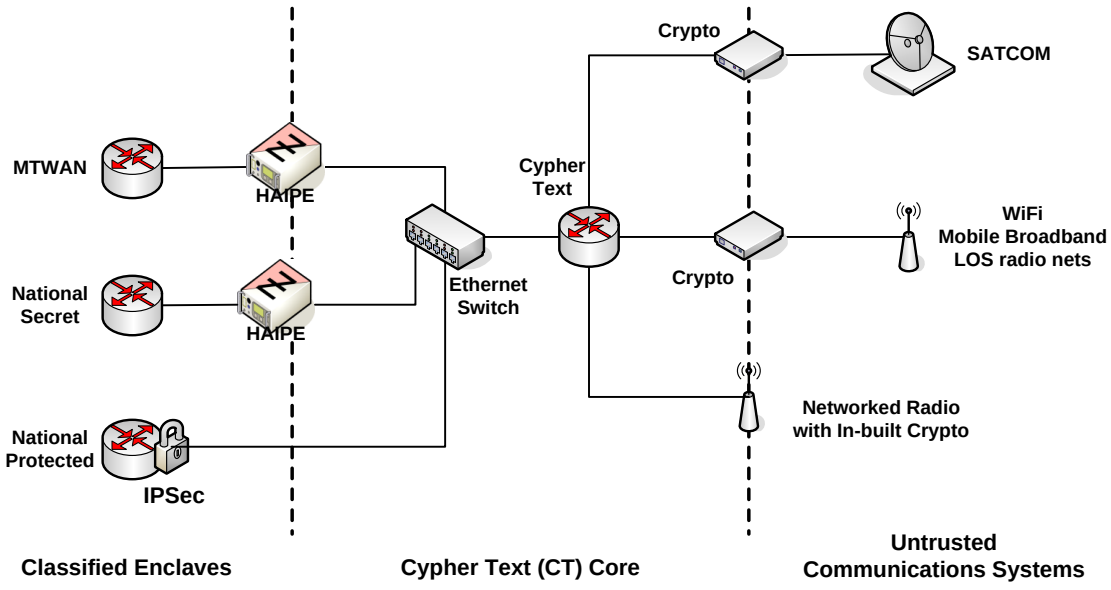

Figure 5A-2 National CT Core Ship Node

13. Some nations have deemed that commercial IPSec or Type 2 encryption is sufficient to protect the core and the transmission of HAIPE Cipher Text over untrusted links. The use of encryptors embedded in commercial routers or modems will need to be approved by national Security Authorities.

14. At the time of writing, SNR has not been integrated with the CT Core because it has not had sufficient bandwidth to support additional VPN overheads and multiple enclaves. However, with an increase in throughput for SNR (known as Wideband SNR) and other potential High Data Rate LOS solutions, it is now practical to integrate the LOS capability with the national CT core to enable ship-ship networking for both national and Coalition enclaves.

NETWORK DESIGN CONSIDERATIONS

15. Link cryptos are transparent to the MTWAN in terms of IP routing, therefore there are no special considerations required in the design of a routing architecture to support legacy architectures that follow traditional single- or multi-Autonomous System (AS) network design.

16. Multi-AS networks such as those of CENTRIXS may be required to support direct ship-ship networking over LOS systems such as SNR, and HFIP between Coalition ships belonging to different AS's using OSPF. Due to the OSPF "backdoor" between the AS's, the routing configuration for these networks is more involved and complex to enable the automatic selection of the most efficient and effective route by a Coalition ship when a change in status of the ship's communications subnets occurs. A routing design to support these multi-AS networks had been developed and validated during previous Trident Warrior periods by A-Z. The design has since been further refined by the US and

adopted for use by CENTRIXS. Details of the design can be found in the Chapter on Routing.

17. It should be noted that the network design for the current CENTRIXS networks CMFP (Coalition Maritime Forces Pacific) and CMFC (Combined Maritime Forces Central) is based on a combination of legacy architecture and a national CT core as shown in Figure 5-4.

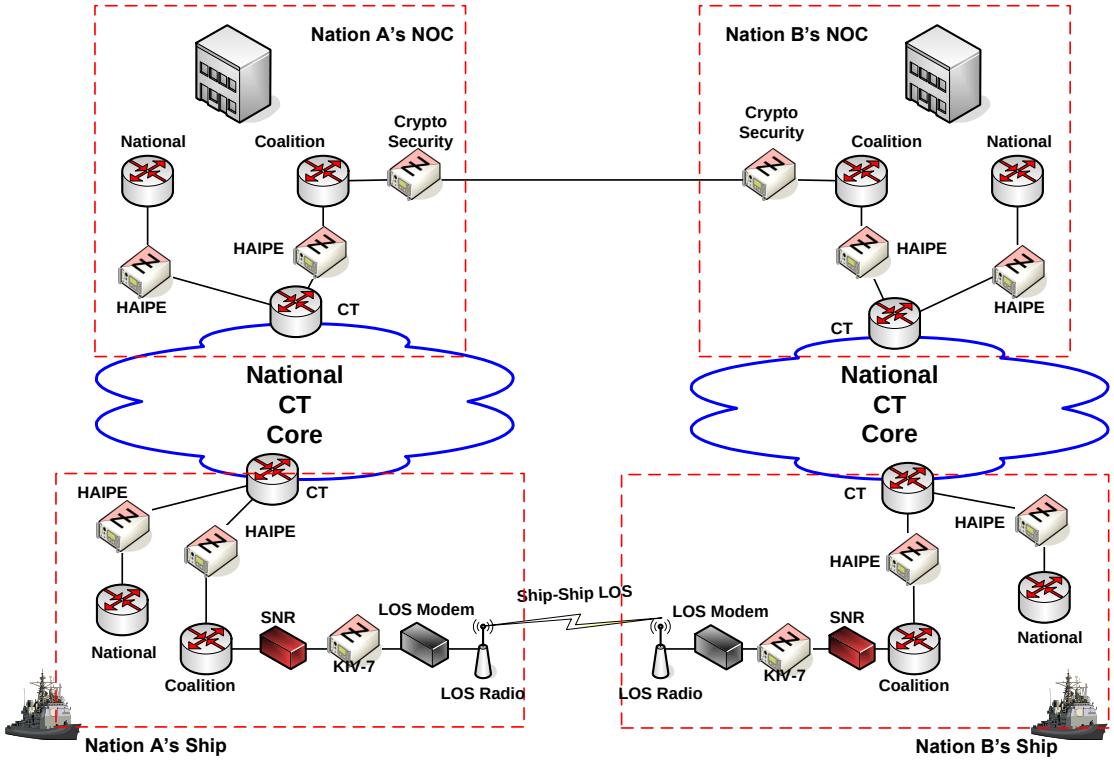

Figure 5A-3 Combination of Legacy Architecture and CT Core

18. CMFP and CMFC are Type-2-protected Community-of-Interest (COI) which use GCTF (Global Counter-Terrorism Forces) network as their transport network, and the GCTF is interfaced with the CT core via HAIPE devices. Figure 5A-5 depicts the IP connectivity for the two COI's in the CT Core.

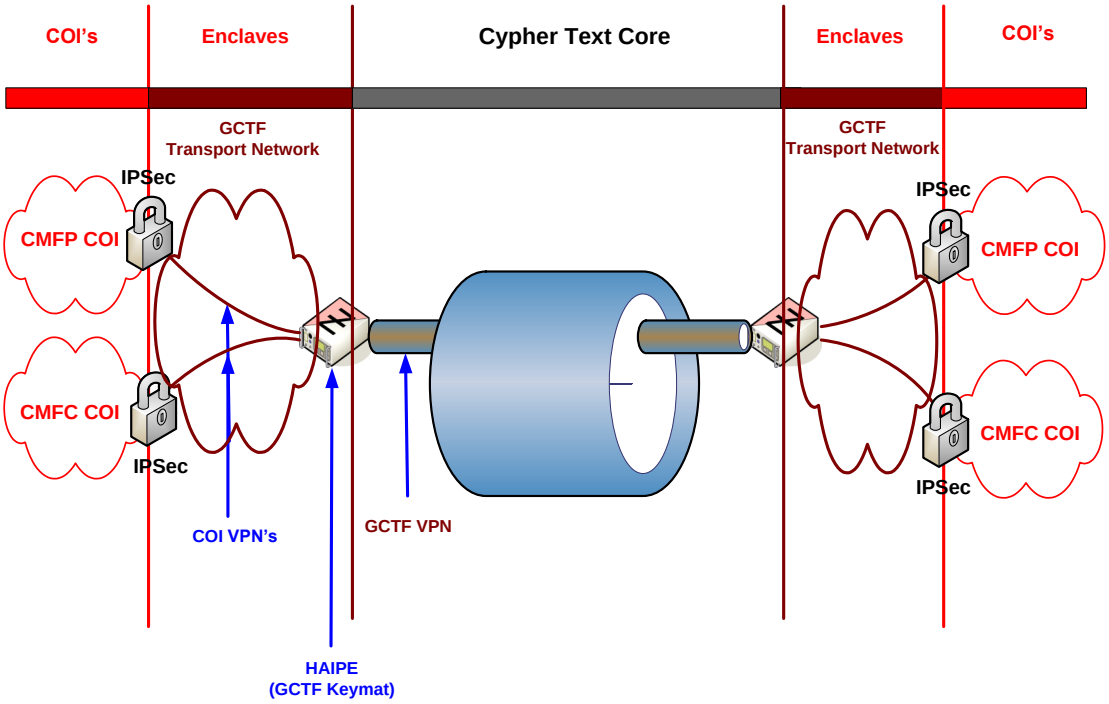

Figure 5A-4 GCTF and COI Virtual Private Networks

19. HAIPE devices interfacing an enclave to the CT core are to be configured for the Tunnel mode operation where an entire IP packet from the enclave will be encrypted to protect not only user information but also network information of the enclave, and then encapsulated into a new IP packet for forwarding to its next destination over the Core.

20. As HAIPE does not support multicast traffic, such as dynamic routing protocol updates very well, the Generic Routing Encapsulation (GRE) protocol will normally be used to encapsulate all data into a unicast packet so that it can be encrypted by HAIPE. However, GRE is a point-to-point connection, therefore GRE-based architectures are not very scalable and are administratively intensive in a fully or partially meshed network.

21. The two technologies mGRE (multipoint Generic Routing Encapsulation) and DMVPN (Dynamic Multipoint VPN) can be leveraged to make the CT core more scalable. New features of HAIPE on Local Discovery, Peer Discovery and Reachability can also be utilised to reduce the reliance on GRE for routing.

22. Another design consideration is the effect on network performance due to VPN and GRE overheads. The encryption and encapsulation will increase the size of the IP packets by up to 85 bytes, which will have some impact on network performance. The use of HAIPE in Tunnel mode and the support for multicast routing updates will result in IP packets from the enclaves arriving at the CT core with three IP headers, two of which are encrypted. Overheads for CMFP and CMFC are even greater. The impact is relatively

small when IP packets are large. However, if the IP packets are too large, they will be fragmented and this will have a detrimental effect on network performance.

23. Some security features of HAIPE, if implemented, can further enhance the security of the network. However their implementation will require careful consideration as they can have dramatic impact on network performance.

CHAPTER 6

NETWORK NAMING AND ADDRESSING

INTRODUCTION

601. There are three important aspects for naming and addressing within a MTWAN: the allocation of IP addresses, the assignment of unique names for the network domains and computers, and the installation and management of Domain Name Service (DNS) servers that support the network.

AIM

602. This chapter defines how names and addresses for entities can be allocated and managed.

OVERVIEW

603. One of the major activities in establishing any mobile tactical network (especially allied and coalition networks) is to identify and promulgate the names and addresses of network elements, including attached end systems and workstations.

604. Addresses should be allocated with attention to the network topology in order to maximise the efficiency of routing information distribution, and hence the data throughput.

605. Any MTWAN DNS has to be linked to the DNS structure of other appropriate national and coalition networks in order to provide address information to-from these other networks.

HOST NAMING CONVENTION

606. The following is recommended to generate the names for individual pieces of equipment (such as computers, printers, routers etc); the host name will be comprised, in order, of the following three fields:

602. Use an abbreviation with a maximum of five letters designating the use of the individual item of equipment, or name of the service which this item of equipment hosts (e.g. COP, Email, DCP) taken from the suggested list at Table 6–1;

603. Type an abbreviation with a maximum of four letters to indicate the type of equipment taken from the mandatory list at Table 6–2;

604. Unique Identifier – a letter of the alphabet (starting at ‘a’), or combination of letters up to 4 letters maximum, used only where necessary to differentiate between two or more machines within a unit which would otherwise have the same name (e.g. pntr-a and pntr-b or pntr-4m and pntr-colr if greater delineation is required).

607. To improve readability, the host name elements are to be separated by a hyphen

("-") (see examples below). If the "Type" component provides sufficient information, for example if there is only one router, then the "Use" component and following hyphen may be dropped. This will most commonly occur with devices, which have only one specific function and are the only one of their kind, e.g. printers and routers.

608. Note that host names cannot begin with a number (i.e. the "use" field of the host name may not start with a number).

609. Tables 6-1 and 6-2 can be amended for specific events (e.g. operations, exercises, demonstrations, trials). However, such amendments will only apply to that event. Devices and conventions that become de facto "Use" and "Type" standards should be submitted for inclusion into ACP 200.

Use Field Abbreviation	Description	Remarks
AUTH	PKI or similar Authentication Service	generally a server
AV	Anti-Virus Service	generally a server
COP	Common Operational Picture/ Recognized Maritime Picture Service	generally a server. e.g. GCCS-M or similar COP service
CT	Cipher-text side of INE device	see INE in TYPE
DCP	Distributed Collaborative Planning	generally a server, e.g. Sametime
DIR	Directory service	generally a server
DNS	Domain Name Service	generally a server
DOM	Domino Web Replication	generally a server
GBS	Global Broadcast System	generally a server
GEN	General Purpose Device	typically a workstation e.g. MS Office
HI	High Side of a Data Diode device	see DIODE in Type
ISSR	Inside Screening Router	Router performing additional packet filtering on incoming network traffic
KEY	PKI or similar Key Server	generally a server
LO	Low Side of a Data Diode device	see DIODE in Type
MAIL	Email or messaging	generally a server
OSSR	Outside Security Screening Router	Router with ingress/egress screening filters
PCHAT	TeamSessions Persistent Chat Service	generally a server
PT	Plain-text side of INE device	see INE in TYPE
TIME	LAN time service generator	generally a server
UHF	For use with UHF LOS and SATCOM networks	see Type
WEB	Traditional Web Service	generally a server
WSUS	Windows Server Update Service	generally a server

Table 6-1 Abbreviations for "Use" Field

Type	Abbreviation	Type Remarks
CAP	Channel Access Processor (CAP)	equivalent to SNAC
CARD	VME Card for MCAP	
CRIU	CAP to Router Interface Unit (CRIU)	equivalent to SRIU
DIODE	Data Diode device	one-way IP data transfer
INE	In-line Network Encryptor	IP encryption device
HFIP	HF IP (STANAG 5066 Ed. 3) gateway	IP over HF; typically a server
HF5066	STANAG 5066 Ed. 1 gateway	email only over HF; typically a server
MLGRD	Mail Guard	
PRNTR	Printer	
ROUT	Router	
SNR	Subnet Relay Network Controller	
SERV	Server	
SNAC	Subnet Access Controller (SNAC)	equivalent to CAP
SRIU	SNAC to Router Interface Unit (SRIU)	equivalent to CRIU
SWIT	Network Switch	
WKST	Workstation PC, X-Terminal, etc.	

Table 6-2 Abbreviations for "Type" Field

610. The following are some examples of the Host Names that can be generated from the above guidance: mail-serv; dom-serv; dcp-serv; cop-serv; gbs-rout; uhf-snr; uhf-cap; gen-wkst-a; gen-wkst-123.

DOMAIN NAMING CONVENTION

611. To generate the names for domains within which the hosts will operate, the domain naming convention shall be composed of elements of the following:

a. Unit – representing the name of the mobile, unit, command or other site;

612. Theatre Commands – represents Theatre / AOR Commands, such as the United States Combatant Commanders (COCOMs);

613. Service – selected from: navy, army, air, marines, joint;

614. Country – the letter country code as defined in ISO 3166 (this may either be the di-graph code described in ISO 3166-2 or the tri-graph code in ISO 3166-3);

615. Enclave – the security enclave of the network;

616. COI – a community of interest (if any) within the enclave;

617. Coalition Military Network Identifier – CMIL; and

618. Military Network Identifier – MIL.

619. The nation or other entity sponsoring a given Allied/Coalition network shall specify in the Network Configuration Plan which of the above naming elements are required for use in that network as well as define the naming. This provides standardization with flexibility of implementation.

620. For CENTRIXS networks, this convention translates to "{ship|unit|command} {3-letter-ISO3166 country-code|cocom} {enclave|enclave-coi}.cmil.mil". Examples of CENTRIXS naming are at Table 6-3.

UNIT		ADDRESS
CMFP COI in GCTF Enclave		
	USS GARY (FFG-51)	ffg51.usa.gctf-cmfp.cmil.mil
	MHQ Australia	mhqaust.aus.gctf-cmfp.cmil.mil
CMFC COI in GCTF Enclave		
	HMNZS TE KAHA	tekaha.nzl.gctf-cnfc.cmil.mil
GCTF Enclave		
	COMPACFLT	cpf.pacom.gctf.cmil.mil

Table 6-3 CENTRIXS Naming

621. The "country code" for NATO is "INT". NATO enclaves include NIDTS, NSWAN, CRONOS, BISCES and LOCE.

622. For temporary, single-enclave activities, the above convention can allow a simpler DNS structure, such as "{ship|unit|command}.service.country". Examples using this simplified naming structure are at Table 6-4.

UNIT	ADDRESS
HMNZS TE MANA	temana.navy.nz
31st MEU	meu31.marines.us
Fleet Injection Point	fip.nato.int

Table 6-4 CENTRIXS Simplified Naming

623. Standard formal National prefixes should not be included in the "unit" portion, as this is implied via the "country" portion. For example, in the case of maritime platforms, unit names are not to include "HMAS", "HMCS", "HMNZS", "HMS" or "USS" etc.

624. Although there are no DNS imposed restrictions on the length of the "Unit" component, for reasons of usability the length for MTWAN purposes should be constrained to 15 characters. Further the DNS entity must be unique within the service and country, e.g. there could be an ottawa.navy.ca, ottawa.navy.us and ottawa.air.ca, but not a second ottawa.navy.ca.

625. As with host names, the domain name cannot begin with a number. In other words, the 'unit' field may not start with a number. Therefore units like 3 CDO BDE will require a lettered prefix. DNS examples for "Numbered Units" are at Table 6-5.

UNIT	ADDRESS
II MEF	us2mef.marines.us
3rd Commando Brigade	uk3cdobde.gbr.cfe.cmil.mil
40th Commando Brigade	uk40cdobde.gbr.gctf-mnfi.cmil.mil

Table 6-5 CENTRIXS Numbered Units

626. Fully Qualified Domain Names (FQDN) are composed of the Host names, whose convention is defined in Paragraph 606 and then the DNS name. Complete FQDN examples are at Table 6-6.

HOST NAME	DNS NAME
Email Server	mail-serv.canterbury.navy.nz
Domino Server	dom-serv.ottawa.can.gctf-cmfp.cmil.mil
Workstation	gen-wkst-b.uk3cdobde.gbr.gctf-cnfc.cmil.mil
GCCS-M Server	gccsm-serv.adelaide.aus.gctf-cnfc.cmil.mil
Router	rout-1.mhqaust.aus.gctf.cmil.mil
TACLANE-cyphertext side	ct-ine-a.3mef.usa.gctf-cnfc.cmil.mil
TACLANE-plaintext side	pt-ine-a.3mef.usa.gctf-cnfc.cmil.mil

Table 6-6 CENTRIXS Fully Qualified Domain Names

ANNEX A TO
CHAPTER 6 TO
ACP 200(D) Vol 2

DOMAIN NAME SERVICE

INTRODUCTION

1. The primary services of DNS are:

   a. Name-to-IP-address mapping;

   b. IP-address-to-name mapping; and

   c. Locating the correct application service hub for any given machine or sub-domain.

2. Applications such as SMTP E-mail, Web Browsers, Chat Clients, etc. are the primary users of DNS. In any particular deployment of an MTWAN, the adopted Domain Name Service (DNS) topology should seamlessly support the host and domain naming structure specified in this document.

AIM

3. This Annex explains how to set up and configure DNS to support an MTWAN.

OVERVIEW

4. Each network host, or more specifically each network interface, has two identifiers: an IP address (which is a 32-bit number) and a Host Name (which is a string). DNS provides forward and reverse mapping between the host name(s) and IP address(es).

5. As applications refer to hosts by names, while packets carry source and destination IP addresses, correct configuration and maintenance of DNS is critical to the effective operation of any IP network.

DOMAIN NAMESPACE

6. The naming system on which DNS is based is a hierarchical and logical tree structure called the *domain namespace*. An example using the CENTRIXS CMFP *unit.service.country.enclave-coi.* is illustrated in Figure 6A-1. This naming schema complies with the naming convention described in Paragraph 10. A tri-graph (i.e. three letter) country code is employed.

7. In this example of DNS hierarchy, first is the Root Server, at the top of the tree. The root server knows the addresses of all authoritative servers in the Domains subordinate to it. This is followed by the Top Level Domain ".mil" which indicates this is a military organization. The Second-level domain ".cmil" indicates this is a Coalition Military network. The Subdomains underneath indicate the specific Coalition enclave, the

nation(s) attached to the enclave, the services of each nation attached to the enclave and finally the units of each service.

8. Each host has both a name and at least one IP address. Applications that run on a host and require name or address resolution will use a resolver to access a DNS server to satisfy the resolution request. The resolver is a set of library routines which are linked to applications to perform the functions of a DNS client.

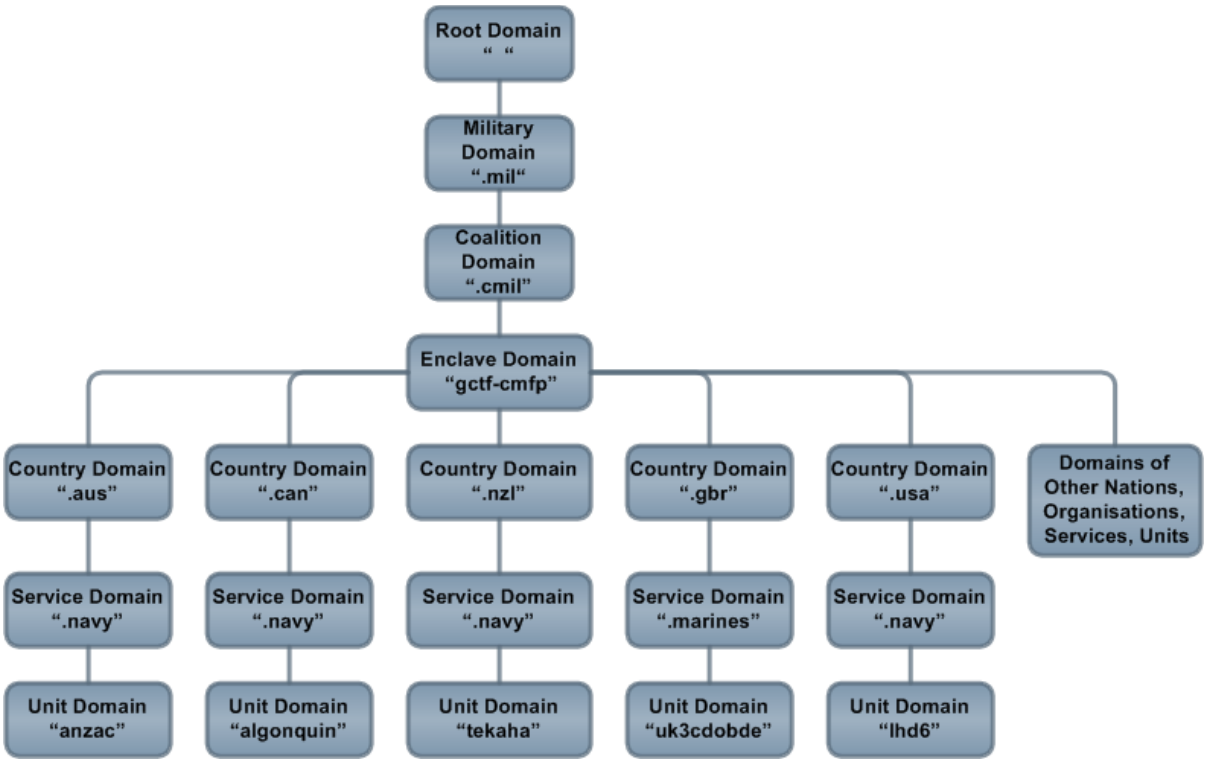

Figure 6A-1 Example Domain Name Service Schema

DNS SERVERS

9. Figure 6A-1 illustrates a typical implementation of DNS for a MTWAN when the MTWAN is connected to a larger network such as CENTRIXS CMFP. DNS servers will be distributed throughout the CMFP WAN. The CWAN host nation will provide the servers for the Top Level domain (".mil"), the Second-Level Coalition Domain ("cmil.mil") and the COI-Enclave Domain ("gctf-cmfp"). Each country will provide servers for its country domain, and also servers for the "service.country" and "unit.service.country" domains. Multiple domains can be supported by a single server. More than one server should be set up for each domain for robustness.

10. There are two types of name servers: primary (also known as master) and secondary (also known as slave). The main difference between the primary and the secondary is

where the server gets its data. A primary server gets its data from files created by users on the host it runs on. A secondary server gets its data over the network from a primary. This is known as a "zone transfer". When a secondary starts up, it loads data from a primary. Once it is operational, it will poll the primary at pre-determined intervals to see if its data is current.

11. For each unit in the MTWAN, the primary DNS server will be located at the MTWAN NOC ashore, and the secondary DNS will be located on the unit as shown in Figure 6A-2. The main purposes of putting the unit's primary DNS server at the NOC is to reduce DNS traffic over the low speed RF nets within the MTWAN and to simplify network administration on ships and other mobile units.

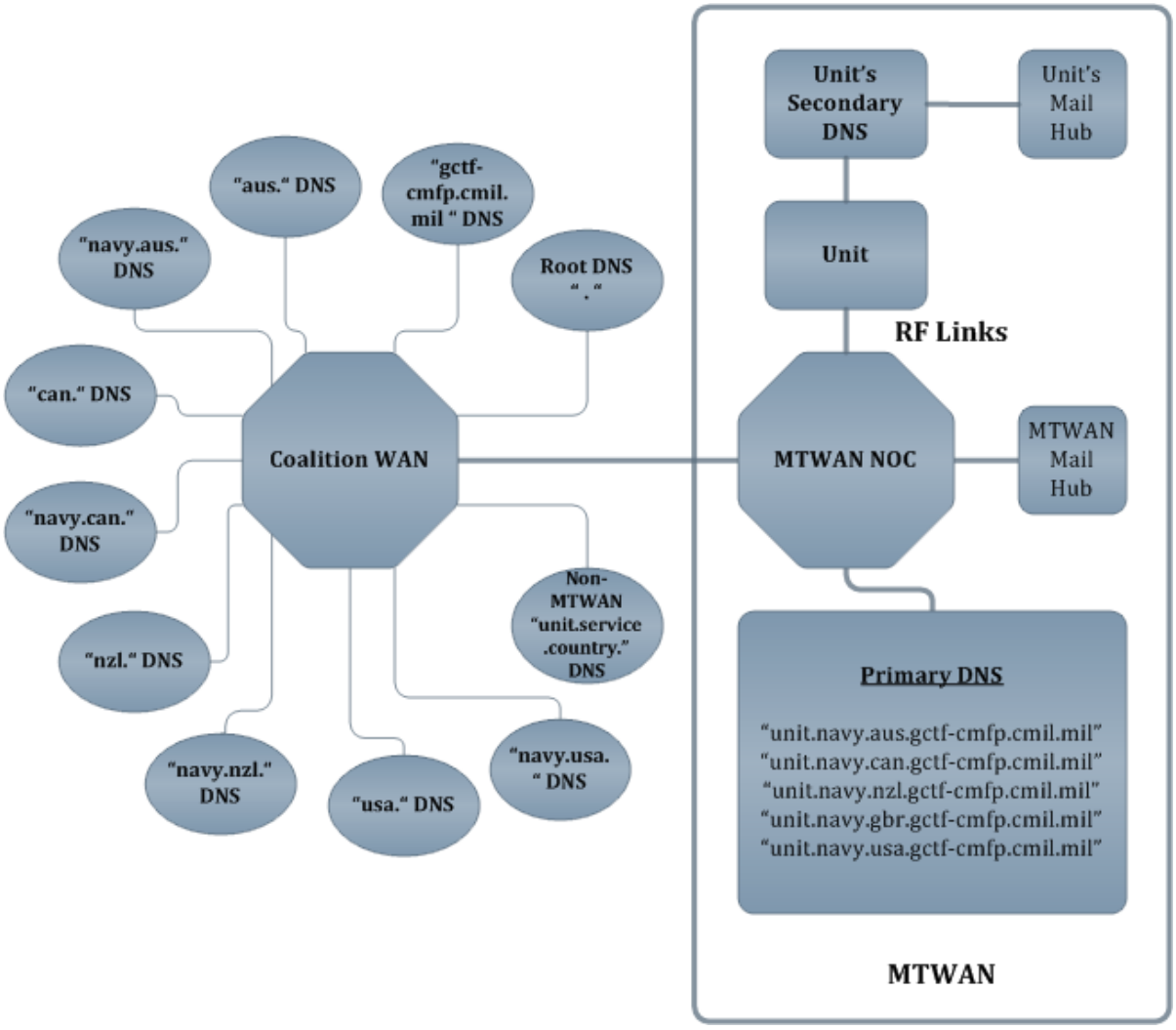

Figure 6A-2 DNS Servers

12. Putting the primary DNS server on the shore reduces DNS traffic over the low speed RF nets because users on the shore-based CWAN can obtain the DNS data from

the shore-based MTWAN DNS server. For example, if a shore-based CMFP user wants to send e-mail to a user on USS BON HOMME RICHARD (LHD-6), the query would be passed to the root DNS servers, the Coalition enclave server ("gctf-cmfp"), the ".usa" server, the "navy.usa" server, and finally the "lhd6.navy.usa" server. All this could occur on land without using the extremely limited RF bandwidth within the MTWAN.

13. Putting the primary DNS server ashore also simplifies network administration onboard the mobile units. DNS requires specially trained network administrators who are familiar with the configuration and maintenance of DNS. By putting the unit's primary DNS on shore, the shore-based engineers can maintain the DNS database, and the unit's DNS server will automatically download the data as required, without intervention by the unit's personnel. When the unit requires changes to the DNS database, it contacts the NOC by voice, chat or electronic mail to request the changes. The NOC will make the requested changes to the db files of the primary server. The updated db files will then be copied by all secondary servers at the next database refresh or at a forced restart of the secondary servers.

14. The disadvantage of having the primary name server for mobile units located at the NOC is that changes to the DNS db files will require the mobiles to send requests for support to the NOC. Units will have to wait until the NOC has modified the shore-based DNS db files and the updated db files have been copied by all the secondary servers before any changes to the DNS will take effect. Where the rate of changes is low, and where there is sufficient advanced DNS planning, this should not be a problem.

15. For operations in environments with limited or no reachback to the NOC, units in the MTWAN will act as secondary DNS servers for all of the other units in the MTWAN. This allows each unit to get DNS information on all other units in one (or a few), efficient bulk transfer transactions, rather than needing a large number of relatively inefficient individual DNS queries.

16. It is recommended that when assembling a MTWAN, consideration is given to combining elements of the DNS name space onto a single DNS server, where such combinations improve efficiency. One area where efficiency can be improved is in careful planning of which national DNS servers can be combined to reduce the amount of network engineering support required at the national level. Another area where efficiencies can be improved is by consolidating multiple mobile units into a single shore-based DNS server. Both of these efficiencies have been successfully employed during previous deployments of the MTWAN.

DNS CLIENTS

17. Hosts on each mobile unit will be configured to refer their DNS queries to the local server. Name-to-address and reverse mapping of an MTWAN host can always be resolved locally, as each unit will act as a secondary server for every other unit. The root servers will only be contacted by the unit's server for mapping of non-MTWAN hosts.

DELEGATION FOR MTWAN SUB-DOMAINS

18. Delegation will be required from the root or parent sub-domain if hosts in the MTWAN sub-domains are to be visible to non-MTWAN hosts. This can be achieved by adding a NS record pointing to the mobile's primary DNS server together with its glue record (a glue record is an A record for a name that appears on the right-hand side of a NS record) to the database of the root or parent DNS server.

19. It is essential that delegation be obtained not only for the name domain but also for the in-addr.arpa domain.

20. Subnetting is used extensively by the MTWAN to make efficient use of the IP address space. As in-addr.arpa sub-domains are organised on IP address byte boundaries, the use of subnetting could complicate in-addr.arpa delegation. Creating database files in this domain should be a straightforward task if delegated zones (a zone is defined as part of the domain delegated to a single server) are on byte boundaries. If a delegated zone is not on a byte boundary but it does not share its in-addr.arpa sub-domain with another zone belonging to a different AS, delegation should also be simple. However, if a node within the MTWAN is to share its in-addr.arpa sub-domain with a non-MTWAN node, special techniques will be required to implement in-addr.arpa delegation across autonomous systems. These techniques are discussed in RFC 2317 entitled "Classless IN-ADDR.ARPA Delegation."

ANNEX B TO
CHAPTER 6 TO
ACP 200(D) Vol 2

SUBNET RELAY AND HIGH FREQUENCY-IP INTERNET PROTOCOL ADDRESSING

INTRODUCTION

1. Subnet Relay (SNR), also known as Mobile Ad-hoc Relay Line-of-sight Network (MARLIN, STANAG 4691), and High Frequency IP (STANAG 5066, Edition 3) provide units with Mobile Ad-hoc Networking capabilities over UHF Line-of-Sight (LOS) and HF Line-of-Sight and Extended-Line-of-Sight (LOS/ELOS) bearers. Proper configuration of IP Addresses is critical for system operation and is facilitated by the IP Addressing schema outlined in this SOP.

AIM

2. This Annex explains how to configure the IP Addressing for SNR/MARLIN and HFIP for operational use.

SNR/MARLIN AND HFIP OVERVIEW

3. Ships in an SNR ad hoc network all use a common, specific UHF radio channel. By design, SNR connects to the router as a layer 2 bridge. The SNR controller is not exposed to the IP layer and so is transparent to OSPF routing. For a given UHF channel the SNR network controller requires each SNR subnet to reside in a Class C address space, providing a single, common entrance/exit into the SNR subnet at Layer 2. This limits the total number of SNR nodes in a single ad hoc network to 253. The IP address of the SCRN Interface can remain constant for all nodes within a given subnet (the 254th Class C IP address).

4. HF IP operates a bit differently from SNR/MARLIN. It connects to the Coalition router as a Layer 3 router with an Ethernet segment. Three IP address are required by the HFIP system; one for the Coalition router interface to the HF IP controller, one for the Ethernet interface on HF IP, and one for the HFIP WAN RF or "over the air" interface. The first two IP addresses must be in the same subnet on each platform, whereas the third must be drawn from a subnet common to all platforms.

5. A /30 netmask is sufficient for the HFIP connection since it has only two endpoints, the ship's Coalition router and the HFIP router. With HFIP, it is possible to utilize Class B IP Addresses and permanently pre-assign IP addresses to each ship, the system does not have the 253 node Class-C IP Address limitation of SNR.

SUBNET RELAY INTERNET PROTOCOL (IP) ADDRESSING PLAN

6. Multiple SNR ad hoc network subnets can be established using multiple UHF channels. IP addresses can be re-utilized in these different subnets as they are separated

by frequency. Care must be taken to coordinate IP Addressing should ships change from one SNR subnet to another in the same geographic area. The details of SNR IP Addressing are contained within the "M2I2 Ad Hoc Routing and Network Paramater Standards v2.0" document.

7. The SNR 253 node limit will not allow all navies to establish a unique SNR IP Address on a given CENTRIXS enclave or COI – no "set it and forget it." A certain amount of re-configuration may be required as ships join up in a given geographic area, particularly for the CNFC and CMFP networks, which have a larger number of participating nations. This reality will require limiting the number of ships per nation that can be "pre-set" in a given enclave or COI.

8. "M2I2 Ad Hoc Routing and Network Paramater Standards v2.0" outlines the allocation of a fixed number of IP addresses within a given enclave or COI for nations to use for deployments. Utilization of these addresses will minimize the amount of IP Address reconfiguration required by NOC and shipboard personnel. The proposed allocations are derived from the maximum number of ships a given nation might surge forward to a given AOR for all but very major combat operations.

9. A small block of IP Address space in an enclave or COI is reserved for the Fleet Commander to allocate as required. Note that IP Address space can be re-utilized if ships are in widely separated geographic areas. For example, Australian ships working up for deployment in the Tasman Sea will not be in the same geographic area as ships in the Arabian Gulf. The geographic separation physically prevents them from joining the same SNR ad hoc network. Use of a Network Configuration Plan which can then be operationally distributed via an OPTASK NET or OPTASK COMMS provides systematic methods for planning.

HF-IP INTERNET PROTOCOL (IP) ADDRESSING PLAN

10. "M2I2 Ad Hoc Routing and Network Paramater Standards v2.0" document delineates the IP Addressing ranges for each CENTRIXS enclave for HF IP controllers.

11. The MTWAN (e.g.CENTRIXS) Router interface and HF IP Router interface (eth0) have 30-bit masks. The HF IP WAN subnet (tap0) has a 28-bit mask. This has been set to limit the number of HFIP nodes within a given HFIP subnet to 15, within a guarded HF frequency. This has been done in order to provide adequate performance for the lower bandwidth HFIP system.

12. Note that the last octet on the HFIP WAN interface is negotiated and automatically assigned to each node by the HF IP network token ring owner.

13. The IP Address assigned to the HF IP WAN subnet (tap0) should be blocked at NOC and ship firewalls. There is no need for this subnet to transit the network.

14. The IP addressing standards and ranges outlined in the document "M2I2 Ad Hoc Routing and Network Paramater Standards v2.0" occupy a generous portion of the IP Address space currently set aside for SNR and HFIP. Most nations will receive a Class C address block, which should cover most, if not all of their potential HF IP installations which can be set and configured once. Fleet Commanders or CoCOMs will also be assigned a Class C block to assign to other nations as required.

15. The "M2I2 Ad Hoc Routing and Network Paramater Standards v2.0" document provides the HFIP addressing schema within the current CENTRIXS enclaves and COI for nations to use and assign. Note that there is room to add additional enclaves as required. Within each enclave or COI, there is IP Address space available to expand should additional nations or nodes need to be added to the overall schema.

CHAPTER 7

OPERATIONAL SERVICES

INTRODUCTION

701. The purpose of an MTWAN is to provide a local mobile network to provide operational services to the user i.e. Web, Chat, Email, Command & Control Applications and the associated data bases and connectivity to ensure they function correctly.

AIM

702. The aim of this chapter is to provide guidance for the provision and management of operational services.

OVERVIEW

703. Operational Services which can be applications, toolsets and associated data bases require configuration and administration in order to ensure they can be used in an effective manner by the user.

APPLICATION MANAGEMENT

704. Operational services and associated data are traditionally hosted and connected through National Network Operations Centres. However, in an MTWAN environment particularly within a satellite denied or degraded environment, the applications will need to be configured in order to continue providing the same operational services.

705. At the network level this will require routing and processes to ensure the operational services are configured to operate dynamically across the MTWAN platform node to node and not rely on National or Primary node services.

706. Each Operational Service comes with its own data management and configuration requirements to work effectively across an MTWAN. The following are generic requirements that have to be considered for the core operational services.

707. Web Applications. Web servers and hosted data should be configured to be replicated across other services on the network.

708. Email. Domain Name Services to ensure mail connectors understand SMTP mail boxes.

709. Situational Awareness. Systems need to be upgraded to include track distribution or management servers i.e. NIRIS or ICS. This then needs to be networked and configured to either automatically distribute managed track sources i.e. Link or Combat System output, or for one node to act as Picture Provider and automatically

distribute to all units on the network.

710. Chat. Chat Servers need to be loaded and configured for automatically or for Chat Applications to be pointed to a centrally provided Chat Server on the network.

CHAPTER 8

NETWORK MANAGEMENT

INTRODUCTION

801. Network Management (NM) is the ability to establish, configure, control, monitor, visualize and prioritize network bearers, devices and the information flow on the MTWAN, in order to ensure that critical information is efficiently and effectively delivered to the warfighter to support the Commander's mission and decision making cycle. NM practices and procedures identified here for the MTWAN can also be employed effectively on other networks and network security enclaves.

AIM

802. This chapter provides guidance for the Network Management of an MTWAN.

OVERVIEW

803. Network Management is more than just the ability to monitor and control the status and health of the various devices and services required to form the network. It includes the development, monitoring and dynamic re-prioritization of a shared situational awareness of the communications, network and applications and services as appropriate to the node, its assigned duties and responsibilities, missions (which will change over time), level of command and so on.

804. The operational effectiveness of a network-centric maritime force depends heavily upon the health of its networks. Thus, it is critical that operational forces from the tactical unit to strategic command have the capability to monitor and assess network status and respond accordingly. The focus must shift from one of fault and performance management, into a larger network management construct that includes the unique challenges of maritime networks. This focus includes the service delivery level as well as the end-to-end prioritization and delivery of critical information.

805. Broader than fault and performance management, is the FCAPS construct: Fault, Configuration, Auditing, Performance, and Security. Auditing is an often overlooked, but necessary, component of NM. Configuration is a major component of day-to-day network management. Equally critical is Security management, which tends to diverge into two distinct communities that perform activities which they describe as NM. "Traditional" network managers tend to focus on configuration and performance. Security managers tend to focus their concerns on intrusion detection and response. Both groups are more or less concerned with fault detection although from different perspectives. Network management must embrace all aspects of FCAPS to be fully effective.

806. The true information exchange requirements on a given node or platform will almost always exceed the capacity of both systems and personnel. This places an operational requirement on Command (at multiple levels) to control information flow.

Proper NM must allow for dynamic information re-prioritization so that the ever changing Critical Information Exchange Requirements (CIER) can be supported as ships and other platforms deploy globally and undergo changes in mission. Network Management must also be cognizant of personnel limitations, including manning, experience, education and other training.

NETWORK MANAGEMENT ARCHITECTURE

807. Ultimately, NM on the MTWAN must seek to bring all afloat and shore infrastructure network and IT devices under a common approach to monitoring and control that can be scaled for use at the NOCs, as well as aboard ships and other maritime platforms. The NM tools deployed in a multi-national network should be able to share customizable views of the network state with the tools employed by other partners. This can be accomplished by either agreeing on the use of a common tool set, or to employ tools which use open or industry standards such as SNMP. Raw and summarized NM data should be made available at all levels of command, while being cognizant of the impact of this data flow on reducing the overall warfare information exchange capability of the MTWAN. National sensitivities in sharing this critical information with partner nations must also be taken into account.

808. NM tools should fuse, filter, correlate, and interpret collected data in displays that are easy to interpret so that operators, administrators and NOC engineers can quickly assess how network bearers, devices and applications/services are performing. NM tools must provide controls for the configuration and tuning of existing network services, and allow quick installation of new services in a controlled manner. Automated controls reacting to dynamic network conditions should be implemented in such a way as to provide service optimization in accordance with mission profiles, in the LAN, MTWAN, regional, and global domains. This allows operators to fine tune prioritization at the application and information/user level to meet the tactical situation.

809. Network Management, which includes monitoring and visualization, traffic management and control, configuration, performance, fault and security management, takes place within maritime platforms, between platforms and throughout the wider enterprise network. NM provides situational awareness on the state of all components of the network, including traffic, and must include knowledge of the following:

a. Status of All communications paths under the node's purview (SATCOM, LOS/BLOS, pier, landline, and local LAN cable plant);

b. Status of network-related cryptographic devices;

c. Status of network hardware, such as routers, switches, servers, workstations, printers and any voice or video devices that may be present;

d. Routing status, including local LAN;

e. Status of processes running on network devices;

f. Applications status, local and remote;

g. Network Security, to include anti-virus/malware alerts on hosts and servers and network intrusion detection alerts;

h. Network configuration, to include operating systems, application versions and patch status;

i. Logging and auditing of network activities;

j. Visualization tools appropriate for both the engineering and operational communities. This could include per-flow application performance;

k. Platform mission(s) to ensure all understand what capabilities are required to be available;

l. Personnel qualifications and capabilities, so that Help Desk and other personnel will be able to assist, or request assistance from them as needed

810. Knowledge and understanding of the state of the entire network allows the most efficient application of node communications and network resources to accomplish a given mission, and to more effectively maintain and troubleshoot network hardware, applications and services. Knowing and understanding the tactical situation and mission of every node is not a realistic expectation for a NOC. A situational awareness (SA) level of understanding of the tactical Information Exchange Requirement for tactical mission success is only available at each node.

811. Network Management requires the ability to visualize the data traversing the MTWAN, on all available bearers, in order to identify the user, the application, destination of data, and the status of network devices. Network management must also include the ability to control the flow of data on the MTWAN in accordance with Command direction (taking platform and any network limitations into account). Network Management must also seek to optimize the approved data stream using various techniques (e.g. compression and acceleration) in order to minimize the actual amount of data traversing the MTWAN bearers.

812. Accomplishing all of this is a complex problem. In visualizing the MTWAN, legacy solutions tend to focus on network health, vice overall information flow. In addition to knowledge of total aggregate traffic and Ports/Protocols (OSI Layer 3 and 4), true Layer 7 visibility is necessary to fully identify and control the data traversing the MTWAN.

813. Network management in a multi-national environment and across security boundaries presents several challenges. Network management tools operate at a single security level and are unable to manage multiple security levels when tunneled through

another security enclave. Network Management across multinational boundaries has many policy-related issues that need to be addressed to ensure national concerns are met.

814. As LOS/ELOS and other ship-ship/ship-air networks become more common on the MTWAN, the warfighter must be provided with the appropriate tools and "best practices" to meet their operational requirements, including tools that can be tailored for the Operational community (e.g. TAO, PWO, ORO, etc.), shipboard administrators and the NOC-based Senior Administrators and engineers.

815. Network Monitoring and Visualization and IA/CND are converging, with both requiring tools that allow the operators and administrators to easily understand and monitor the MTWAN, provide the necessary Indicators and Warnings regarding MTWAN health, and response capabilities for any undesired network activities. As mentioned above there are two distinct communities, each of which believes they are charged with N: the "traditional" device and application performance/fault monitoring community and the IA/CND community, which focuses on intrusion detection and response. Ultimately, both groups are seeking after fault detection and remediation to ensure the integrity of the network, its devices and the information flowing through it, albeit from two different perspectives. Both groups should be able to operate using a common toolset to perform their respective mission goals and objectives.

NETWORK OPERATIONS CENTRES (NOCS)

816. From an enterprise WAN perspective, NM is commonly associated with the duties and responsibilities of a Network Operations Centre (NOC). A NOC, while logically in one location, could physically be in a number of locations (i.e. distributed in nature). Depending on the design of the MTWAN, there will likely be a number of NOCs. There will normally be three types of NOCs on the MTWAN: the Primary NOC, National NOCs, and maritime units or other nodes that will have NOC-like duties and responsibilities. The latter is an emerging requirement that allows ships and Task Groups to continue operations in SATCOM-Restricted or SATCOM-Denied environments.

817. An MTWAN is an international network combining networks of member nations. Each member has a national NOC to undertake independent network management, with management of the overall network undertaken by a Primary NOC. To act as a "NOC Afloat," maritime units must have capabilities similar to those of the NOC in order to properly administer and maintain the network when shore reachback is not possible.

818. Each national NOC communicates to each other through a secure core network allowing communication between nodes of differing nationalities.

819. The MTWAN NOC or Primary NOC generally provides a single point of contact for network services within a mobile tactical network. The provision of services to this network and for coordinating connectivity of national NOCs to the network is a MTWAN NOC responsibility. With the advent of ship-ship networking, both the MTWAN NOC

and National NOCs must be capable of relaying traffic arriving from other nations who may not have connectivity to their national NOC.

820. The National NOCs are responsible for coordinating network services within their national boundaries and to coordinate activities with the primary NOC. They provide a critical line of defense for networks afloat, as well as host applications and services. National NOCs must be capable of relaying traffic arriving from other nations whose maritime units may not have connectivity to their national NOC and are relaying through another ship using LOS/BLOS networks (e.g. Subnet Relay).

PLATFORM LEVEL

821. Individual nodes are responsible for management of local network elements in addition to the tactical prioritization of information inbound and outbound from their node. Each platform must have a capability to provide network management services and OSI Layer 7 information prioritization for their LAN as well as the MTWAN. SATCOM-Restricted or SATCOM-Denied environments will cause one or more platforms to become a "NOC Afloat," and provide one or more services for the Task Group. These nodes are responsible first to the national NOC and then the primary NOC for overall network services.

822. Platforms equipped with ship-ship or other LOS/ELOS networking capabilities must be capable of hosting and administering critical applications and services in the event of SATCOM loss. This is a shift from the NOC-centric to a Task Group-centric environment. Depending upon mission and capabilities, one or more ships may be designated as the "NOC Afloat." Members of the Task Group would access these services (e.g. Chat) on the designated "NOC Afloat" platform directly via ship-ship networking. NM tools and capabilities also need to be present on ships so that they can appropriately administer the MTWAN.

MTWAN NETWORK MANAGEMENT

823. MTWAN Network Management is achieved throughout the production and distribution of a Network Configuration Plan, of which the details and composition are in Chapter 9. This is a very detailed and comprehensive document intended for NOC / Node management of the services. The operational network management information is distributed into the tactical environment through the formatted message OPTASK NET, of which details and composition are in Chapter 9 Annex A.

NETWORK MANAGEMENT ELEMENTS

824. The elements of network management are:

a. Configuration Management that controls the behaviour of the network and can be considered to comprise of upgrades, repairs and equipment or services replacement. Also involves corrective preventive measures and auditing;

b. Configuration, monitoring and control of all communications systems carrying IP traffic under the purview of a given node, to include provisioning and bandwidth management, to include SATCOM, LOS/ELOS and pierside connectivity;

c. Configuration, monitoring and control of all cryptographic systems protecting IP traffic under the purview of a given node;

d. Configuration, monitoring and control of routers and other Simple Network Management Protocol (SNMP)-managed network devices, including those of the local LAN and the MTWAN;

e. Route Policy Management (which networks carry transit traffic, diversity routing, tunneling and overlay network management, security service levels for routing protocols);

f. Administration Management of DNS, Email, Web, network time service, and other required infrastructure applications and services, both local and remote;

g. Operations Management of the network to maintain services, which includes real-time monitoring and resolution of issues. This must include visualization tools that are appropriate for both the engineering and operational communities;

h. Security Management as covered by Chapter 5;

i. Platform mission(s) and changes to those missions over time; and

j. Personnel qualifications and capabilities at a given node or platform.

825. To accomplish the above, NM requires the platform to monitor and assess the performance of the network hardware, software, and media, and includes:

a. Monitoring of Links, Routers, network connectivity and Services;

b. Net loading, congestion control monitoring;

c. Performance optimisation for bandwidth-disadvantaged users;

d. Service Prioritisation;

e. Fault Management;

f. Fault detection, isolation and troubleshooting;

g. Fault-logging and analysis;

h. Local System Administrators;

i. Local network monitoring;

j. Monitoring and reporting of the local and MTWAN Information;

k. Assurance and Computer Network Defence posture; and

l. Predictive monitoring

826. Visualization of the NM information should include easy to use interfaces and displays tailored not only for the Administration/Engineering community, but also for the Operational community. Platform and MTWAN status is a large factor in how one would "fight the ship."

827. Often, the primary source of insight the NOC has into shipboard network health is through network trouble tickets, generated via phone calls from ship to shore seeking technical assistance. Proper NM on the MTWAN requires improved cross-integration of both platform and NOCs. Maritime platforms must be able to provide current network information and status to the shore and NOCs. The shore and NOCs must be more proactive in addressing operational problems on the MTWAN. Enterprise-wide Network Operations (NETOPS) for the MTWAN are available from national and multi-national sources and provide an excellent CONOPS as a guide.

ACCOUNTING AND AUDITING

828. Proper accounting and auditing is important in the overall network management of the MTWAN. Users must be held responsible for their actions in a computer system. Users can be authorized to access a resource; and if they access it, the operating system or application needs to provide an audit trail that gives historical data on when and how a user accessed a given resource. Conversely, if a user tries to access a resource and is not allowed to do so, an audit trail is still required to determine if an attempt was made to violate system authorization and, in some cases, authentication policies.

829. Accounting is the process of maintaining an audit trail for user actions on the system. Accounting may be useful from a security perspective to determine authorized or unauthorized actions; it may also provide information for successful and unsuccessful authentication to the system. Accounting should be provided, regardless of whether or not successful authentication or authorization has already taken place. A user may or may not

have been able to authenticate to the system, and accounting should provide an audit trail of both successful and unsuccessful attempts.

830. Furthermore, if a user has managed to authenticate successfully and tries to access a resource, both successful and unsuccessful attempts should be monitored by the system; access attempts and their status should appear in the audit trail files. If authorization to access a resource was successful, the user ID of the user who accessed the resource should be provided in the audit trail to allow system administrators to track access.

831. The accounting and auditing processes, and associated information, feed into the overall MTWAN IA/CND processes.

TOOLS

832. Multiple tools are available that facilitate network status and traffic load monitoring, as well as tools using SNMP to implement centralized or remote control of network elements. However, no single tool as yet provides all of the desired capabilities. Because of constrained bandwidth between ship and shore, SNMP queries from shore managers to shipboard systems are not likely to provide a workable solution into a broader network Situational Awareness. This is also true of systems, and tools designed for high-bandwidth terrestrial enterprise networks will be risky endeavors. NM tools must be implemented to minimize their bandwidth impact on the MTWAN.

833. All platforms should, as a minimum, have the ability to monitor local and MTWAN network status and traffic performance. All platforms should, as a minimum, have the ability to monitor local and MTWAN network status and information exchange performance. Ideally, all platforms should have the ability to monitor all networked information to the application; identified and associated with every user request and response, along with the ability to prioritize those information requests to both application and user.

NETWORK MANAGEMENT AND QUALITY OF SERVICE (QOS)

834. NM should take advantage of QoS, particularly at the platform level. Maritime platforms typically do not enjoy the high bandwidth and low latencies of terrestrial networks. Network congestion has compelled nations to deploy traffic shaping and QoS appliances to control outbound traffic. With today's complex information environments, the focus of congestion control has increasingly shifted to the traffic flowing inbound to the platform. With maritime assets being deployed on a wide variety of missions around the world, National NOC's have very little situational awareness (SA) at the operational level and almost none at the tactical level of warfare. Global outbound QoS settings provide a basic framework, but tactical QoS (fine tuning) is best handled by the platform at sea.

835. Two significant trends are driving the need for a shift to inbound QoS. One trend is the adoption of mesh network technologies which enable routing of application traffic

directly from one platform to another over LOS bearers, without requiring NOC reachback. The second drive is the emergence of Software as a Service (SaaS) applications and cloud services, with data incoming from both national and international data centers, and may reach the platform via multiple WAN paths. To ensure that critical applications perform predictably with a high level of performance it is essential to control less important traffic and to make room on the network for vital data to get through. For National Restricted Networks, applications and websites accessed over the Internet compete for bandwidth with recreational traffic, meaning corporate enterprise web based applications may struggle for needed resources. Placing devices at third-party websites to do outbound QoS is generally not an option, making the point at which traffic enters the at sea platform the only possible place to adequately control bandwidth usage.

836. Inbound QoS provides the tactical platform with the means to determine how their tactical information links will be used. It allows command to prioritize all information coming into the ship across the networks in order to ensure the dynamic tactical information requirements and restrictions (INFOSEC/OPSEC) are met to help ensure mission success. Inbound QoS differs subtly from outbound QoS in that it occurs after traffic has traversed the MTWAN, and after the traffic has gone through a network bottleneck.

837. Inbound QoS requires that the inbound traffic control solution be the point at which traffic is queued. Network traffic arriving on-site after being rate-limited by an upstream router renders the QoS solution implemented at the receiving location ineffective. The upstream bottleneck is commonly an unmanaged first-in-first-out (FIFO) queue that gives no consideration to the determined business requirements of the receiving organization, which negatively impacts the performance of latency-sensitive applications, such as VoIP.

838. For an inbound QoS solution to be the authoritative control point for traffic entering a platform, it must employ unique techniques to ensure it solely plays the role of traffic shaper. Several key mechanisms help to ensure that incoming applications are accurately controlled and given the bandwidth and priority needed to match the identified requirements of the organization, and include TCP control, flow padding and link padding. TCP control smooths out TCP microbursts via small scheduling adjustments at well-chosen times so that slow-starting TCP flows remain below the bottleneck rate. Flow padding makes room for new flows, and is a form of short-term bandwidth reservation done on a per-flow basis that takes advantage of standard TCP congestion control behavior to help shape traffic. Link padding reserves a small, fixed amount of the available bandwidth to ensure the inbound QoS solution is the bottleneck for the traffic that it is scheduling and creates opportunity to shape traffic because it sees traffic arriving at or below the line rate.

839. Inbound control requires careful orchestration of the competing priorities and behaviors of application flows. Solutions that feature advanced inbound control technology ensure each application gets the right level of service across the network.

840. This capability paired with intelligent traffic identification and scheduling that takes into account not just bandwidth allocation, but also the sensitivity of a given application to latency, allows warfare applications to perform predictably when delivered over the MTWAN as well LOS bearers.

GENERATION OF REPORTS

841. An MTWAN NOC, or designated NOC-Afloat, will provide network status information to the CTG Commander, to Task Group members and to the higher level Allied WAN management system. This information must be kept current and be presented as a Web page.

842. To enable an MTWAN NOC to collect, collate and disseminate the latest status information, all platform network managers are to provide local status reports on a regular basis (or at least, when there has been any change since the last report). The NOC will compile these into an overall status report.

843. Deviations from the published Network Configuration Plan and/or the OPTASK NET must be shared with all members of the network as quickly as possible, with updates to those documents as appropriate.

844. An enterprise-wide understanding of MTWAN health can only be accomplished integrating both the bottom-up reporting by individual platforms on their network and MTWAN status, as well as the top-down view provided by the NOC.

CHAPTER 9

NETWORK CONFIGURATION PLAN (NCP)

INTRODUCTION

901. The management of the MTWAN requires that the network be designed and documented to allow nations to efficiently and effectively configure their respective components of the AMTWAN. In the Coalition mobile environment the Network Configuration Plan is used to promulgate the required network configuration information to participating nations: the OPTASK Net is the formal message derived from the NCP for ease of military distribution.

AIM

902. The aim of this chapter is to amplify the NCP and OPTASK NET and provide an example of its content. The format for the creation of the NCP is included at Annex A. The OPTASK NET is a formatted message that will provide the option for systems that are capable to conduct, transfer and output via XML tagging.

RESPONSIBILITY

903. High-level network configuration information will normally be provided in the NCP. The NCP is normally developed by the national delegated authority and may be published as an Appendix to the OPLAN or issued as a separate document if required.

904. Using this higher level guidance, the local Commander may detail specific tactical level requirements in the OPTASK NET. The creation of these documents requires close liaison with participating nations and their Network Operating Centers (NOCs) in order to achieve an accurate final document.

CLASSIFICATION

905. Where possible, the NCP should be kept at the UNCLASSIFIED level until such time as the document is populated and becomes approved for use. This will allow rapid collaboration with nations for its creation.

906. In its final format, the NCP and / or the OPTASK NET should be classified as appropriate for the Operation or Exercise, with the appropriate releasability caveats.

FORMAT

907. Due to the nature of the contents of the NCP, it does not lend itself to the Maritime Tactical Format (MTF). During the collaboration phase with participating nations, the preferred format is a MS Word document format. The preferred final format is the Portable Document Format (PDF) file format.

TABLE OF CONTENTS

908. The NCP should contain the following, although this is not an exhaustive list and will depend upon the associated operation or exercise.

a. OBJECTIVE.

b. ADMINISTRATION.

(1) PERIOD.
(2) SCOPE.
(3) CHANGE MANAGEMENT.
(4) REFERENCES.

c. DUTIES AND CONTACT INFORMATION.

(1) COALITION TECHNICAL COORDINATOR.
(2) MTWAN NETWORK MANAGERS.
(3) NATIONAL NOC TROUBLE/ HELP DESKS.
(4) UNIT/SITE NETWORK MANAGERS.
(5) APPLICATIONS AND TECHNOLOGIES POCS.

d. ARCHITECTURE.

(1) DESCRIPTION OF ENCLAVES.
(2) SYSTEM SECURITY LEVEL.
(3) CROSS DOMAIN CONNECTIONS.

e. MTWAN BEARERS.

(1) TERRESTRIAL.
(2) MILITARY SATCOM.
(3) CIVILIAN SATCOM.
(4) HF.
(5) UHF.

f. ROUTING.

(1) NETWORK ROUTING TOPOLOGY.
(2) ROUTING PROTOCALS AND PARAMETERS.
(3) NATIONAL NODE CONFIGURATIONS / IP ADDRESSING.

g. NETWORK APPLIANCES QOS.

(1) PACKET MARKING AND HANDLING.
(2) WAN OPTIMISATION.

h. SECURITY.

(1) LINK ENCRYPTION.
(2) IP ENCRYPTION.
(3) FIREWALLS.
(4) INTRUSION DETECTION SYSTEMS.

i. DOMAIN NAME SERVICES

j. APPLICATIONS.

(1) COP.
(2) EMAIL.
(3) CHAT.
(4) COLLABORATION WORKING.
(5) VOIP.
(6) OPERATIONAL STAFF WORK.

k. NETWORK MANAGEMENT

l. ADDITIONAL INFORMATION

m. SUMMARY

OPTASK NET

909. The OPTASK NET will be derived from the NCP normally in a formatted text in order to portray the information over military systems. The formatted textual format is at Anenx A.

OPTASK NET

Message identifier (Name): OPTASK NET (Operational Tasking for a Mobile Tactical Network)

Related Documents: ACP 200

Purpose: The purpose of the OPTASK NET is to provide front line units with the specific setting for their unit which differ from those in the Network Configuration Plan (NCP) or that are required in addition to those found in the NCP.

Sponsor: Navy Command

Notes: None

Status: Editing

KEY:✓= Repeatability**, M**= Mandatory, **C**= Conditional, **O**= Operationally Determined, **#**= only 1 of the alternatives MAY be selected,*****= One or more alternatives MUST be selected. **Alt with no symbol**= only 1 of the alternatives MUST be selected

Seg	Alt	Rpt	Occ	SETID	Seq	Set Format Name	Description
			O	**EXER**	1	EXERCISE IDENTIFICATION	IDENTIFIES THE EXERCISE THE MESSAGE PERTAINS TO. NOT TO BE USED IN CONJUNCTION WITH SET OPER.
			C	**OPER**	2	OPERATION CODEWORD	IDENTIFIES THE OPERATION THE MESSAGE PERTAINS TO. NOT TO BE USED IN CONJUNCTION WITH SET EXER.
SET 2 (OPER) IS PROHIBITED IF SET 1 (EXER) OCCURS.							

Seg	Alt	Rpt	Occ	SETID	Seq	Set Format Name	Description
			M	MSGID	3	MESSAGE IDENTIFIER	Specifies identifying details regarding a document, image or other information exchange media that is applicable to the content of this message. The values of Field 1 must be completed exactly as specified in the structural relationship rule.
FIELD 1 IN SET 3 (MSGID) IS ASSIGNED THE VALUE "OPTASK NET".							
			O	REF	4	REFERENCE	Specifies identifying details regarding a document, image or other information exchange media that is applicable to the content of this message.
			M	PERIOD	5	PERIOD OF TIME	Specifies the period of time for which the OPSTAT UNIT is effective.
			O	POCDATA	6	MTWAN MANAGER	Provide the contact information for the MTWAN Manager.

[1.1] Start of OPERATIONALLY DETERMINED Segment SYSTEM SETUP INFORMATION which MAY be repeated (unlimited times).
The segment groups all information about a system together.
This Segment may contain the following nested Segment(s) [1.1.1] UNIT SETTING

Seg	Alt	Rpt	Occ	SETID	Seq	Set Format Name	Description
1.1			M	SYSTEM	7	IP SYSTEM	Provides the name of the system that the remainder of the segment refers to.
1.1		✓	M	MTWANSET	8	MTWAN BEARER	Provides the setting date for a MTWAN Bearer. This set should be repeated for each bearer.

[1.1.1] Start of OPERATIONALLY DETERMINED Segment UNIT SETTING which MAY be repeated (unlimited times).
Provides the settings for individul units.

Seg	Alt	Rpt	Occ	SETID	Seq	Set Format Name	Description
1.1.1			M	UNITIP	9	UNIT IP SETTINGS	Provides information about the Internet Protocol settings for a unit.
1.1.1		✓	O	UNITSVC	10	UNIT SERVICE	Provides information about each of the network services that are provided by the unit. The set is repeated for each service.

[1.1.1] End of UNIT SETTING

Seg	Alt	Rpt	Occ	SETID	Seq	Set Format Name	Description
1.1			O	GENTEXT	11	ADDITIONAL SYSTEM INFORMATION	Provide additional information about the system.
FIELD 1 IN SET 11 (GENTEXT) IS ASSIGNED THE VALUE "ADDITIONAL SYSTEM INFORMATION".							

[1.1] End of SYSTEM SETUP INFORMATION

AMPN

Set identifier (Name): AMPN (AMPLIFICATION)

	FREE TEXT M		
AMPN	/	1-Unbounded	//

No	Designator	Field Desc	Concept/Explanation/Examples
1	**FREE TEXT**		
	1A FREE TEXT		ENTER IN FREE TEXT THE INFORMATION TO AMPLIFY THE IMMEDIATELY PRECEDING SET. See table **1006/1** which is an instructive entry

Notes: none

Related Documents: none

Examples:

```
AMPN/ACFT REQUIRED AT 4HRS GROUND ALERT AT
OERLAND DURING ENTIRE
PERIOD OF EXERCISE//
```

Specific Requirements:: none

EXER

Set identifier (Name): EXER (EXERCISE IDENTIFICATION)

	EXERCISE NICKNAME		EXERCISE ADDITIONAL IDENTIFIER		
	M		O		
EXER	/	1-56	/	4-16	/ /

No	Designator	Field Desc	Concept/Explanation/Examples
1	**EXERCISE NICKNAME** 1A EXERCISE NICKNAME		ENTER THE CODE NAME OR NICKNAME OF THE EXERCISE TO WHICH THE MESSAGE PERTAINS, FOR EXAMPLE: "CMX 95". See table **1021/1** which is an instructive entry
2	**EXERCISE ADDITIONAL IDENTIFIER** 2A EXERCISE ADDITIONAL IDENTIFIER		ENTER THE ADDITIONAL EXERCISE NICKNAME IDENTIFIER FROM NADREX PART I, CHP 3, FOR EXAMPLE: "CONTROL". See table **1018/11** which contains a list of data items and associated data codes

Notes: none

Related Documents: none

Examples: `EXER/CMX 95/CONTROL//`

Specific Requirements:: none

GENTEXT

Set identifier (Name): GENTEXT (GENERAL TEXT)

	TEXT INDICATOR		FREE TEXT		
	M		M		
GENTEXT	/	1-61	/	1-Unbounded	//

No	Designator	Field Desc	Concept/Explanation/Examples
1	**TEXT INDICATOR** 1A TEXT INDICATOR		ENTER THE REPLACEMENT NAME THAT IS REQUIRED FOR THIS SET, FOR EXAMPLE: "COMMANDERS ASSESSMENT". See table **1009/1** which is an instructive entry
2	**FREE TEXT** 2A FREE TEXT		ENTER IN FREE TEXT OF AN UNLIMITED NUMBER OF CHARACTERS THE COMMENTS THAT YOU WISH TO SEND TO THE OTHER END. See table **1006/1** which is an instructive entry

Notes: none

Related Documents: none

Examples:

```
GENTEXT/COMMANDERS ASSESSMENT/HERE YOU MAY ADD
ANY COMMENTS IN FREE
TEXT OF AN UNLIMITED NUMBER OF CHARACTERS THAT IS
REQUIRED BY THE
MESSAGE//
```

Specific Requirements:: none

MSGID

Set identifier (Name): MSGID (MESSAGE IDENTIFIER)

	MESSAGE TEXT FORMAT IDENTIFIER M		ORIGINATOR M		MESSAGE SERIAL NUMBER O		MONTH NAME O		QUALIFIER O		SERIAL NUMBER OF QUALIFIER O		
MSGID	/	1-32	/	1-30	/	1-13	/	3-3	/	3-3	/	1-3	//

No	Designator		Field Desc	Concept/Explanation/Examples
1	**MESSAGE TEXT FORMAT IDENTIFIER**			
	1A	MESSAGE TEXT FORMAT IDENTIFIER		ENTER THE MESSAGE TEXT FORMAT IDENTIFIER, FOR EXAMPLE: "OPTASK NET". See table **1018/2** which is an instructive entry
2	**ORIGINATOR**			
	2A	ORIGINATOR		ENTER THE MESSAGE ORIGINATOR (NORMALLY IN THE SHORT OR STANDARD ABBREVIATED FORM), FOR EXAMPLE: "SHAPE". See table **1029/1** which is an instructive entry
3	**MESSAGE SERIAL NUMBER**			
	3A	MESSAGE SERIAL NUMBER		ENTER THE MESSAGE SERIAL NUMBER (NUMBERING WILL BE ACCORDING TO THE INSTRUCTIONS OF THE HQS OR FORMATION CONCERNED), FOR EXAMPLE: "15". See table **1012/7** which is a range [0 through 9999999999999]

No	Designator	Field Desc	Concept/Explanation/Examples
4	**MONTH NAME** 4A MONTH NAME		ENTER THE MONTH STANDARD 3-LETTER ABBREVIATION, FOR EXAMPLE: "DEC". See table **1004/1** which contains a list of data items and associated data codes
5	**QUALIFIER** 5A QUALIFIER		ENTER THE CODE WHICH CAVEATS THE MESSAGE STATUS, FOR EXAMPLE: "PER". See table **1130/3** which contains a list of data items and associated data codes
6	**SERIAL NUMBER OF QUALIFIER** 6A SERIAL NUMBER OF QUALIFIER		ENTER THE QUALIFIER SERIAL NUMBER (SERIALLY STARTING WITH 1 FOR FIRST QUALIFIER TO ANY MESSAGE), FOR EXAMPLE: "5". See table **1012/29** which is a range [1 through 999]

Notes: none

Related Documents: none

Examples: `MSGID/XXXXX...../SHAPE/15/DEC/PER/5//`
`MSGID/XXXXX...../SHAPE/-/-/PER//`

Specific Requirements:: none

MTWANSET

Set identifier (Name): MTWANSET (MOBILE TACTICAL WIDE AREA NETWORK SETINGS)

	BEARER		WAVE FORM		DATA RATE		CRYPTOGRAPHIC HARDWARE		KEYMAT		FREQUENCY	
	M		M		M		M		M		O	
MTWANSET	/	1-24	/	3-25	/	4-16	/	1-16	/	8-10	/	3-25

	TIME SOURCE		
	M		
MTWANSET	/	1-64	//

No	Designator		Field Desc	Concept/Explanation/Examples
1	**BEARER**			**Specifies the bearer that the settings apply to.**
	1A	Wide Area Network Bearer		Enter the name of the bearer, for example: "HD SNR". See table **1275/900** which contains a list of data items and associated data codes
	1B	Generic Bearer	OTH	Enter "OTH:" followed by the name of a bearer that is not available from the list for Alt A, for example: "7G". See table **1275/901** which is an instructive entry
2	**WAVE FORM**			**Specifies the wave form that is to be set for use on the bearer.**
	2A	WAVE FORM		Enter the waveform frequency, for example: "25KHZ". See table **2064** which is a composite
3	**DATA RATE**			**Specifies the data rate to be set.**
	3A	DATA RATE		Enter the data rate, for example: "123.5MBPS". See table **2501** which is a composite

No	Designator	Field Desc	Concept/Explanation/Examples
4	**CRYPTOGRAPHIC HARDWARE**		**Specifies the cryptographic hardware that is to be used.**
	4A TYPE OF CRYPTOGRAPHIC EQUIPMENT		Enter the type of cryptographic hardware, for example: "KB93B" See table **1135/18** which is an instructive entry
5	**KEYMAT**		**Specifies the KEYMAT to be used.**
	5A CRYPTO KEYING MATERIAL		Enter the KEYMAT publication number, for example: "ABCS123". See table **1078/4** which is an instructive entry
6	**FREQUENCY**		**Specifies the bearer frequency.**
	6A RADIO FREQUENCY		Enter the frequency, for example: “123.501KHZ” See table **2064** which is a composite
7	**TIME SOURCE**		**Specify the time source for the bearer.**
	7A TIME SOURCE		Enter the time source, for example: "ntp.usno.navy.mil". See table **1022/801** which is an instructive entry

Notes: none

Related Documents: none

Examples: `MTWANSET/HD SNR/25KHZ/123MBPS/KB93B/ABCS123A/243MHZ /ntp.usno.navy.mil//`

Specific Requirements:: none

NARR

Set identifier (Name): NARR (NARRATIVE)

	FREE TEXT M		
NARR	/	1-Unbounded	//

No	Designator	Field Desc	Concept/Explanation/Examples
1	**FREE TEXT**		
	1A FREE TEXT		ENTER IN FREE TEXT THE INFORMATION TO AMPLIFY THE IMMEDIATELY PRECEDING GROUP OF SETS. See table **1006/1** which is an instructive entry

Notes: none

Related Documents: none

Examples:

```
NARR/ACFT REQUIRED AT 4HRS GROUND ALERT AT
OERLAND DURING ENTIRE
PERIOD OF EXERCISE//
```

Specific Requirements:: none

OPER

Set identifier (Name): OPER (OPERATION CODEWORD)

	OPERATION CODEWORD		PLAN ORIGINATOR AND NUMBER		OPTION NICKNAME		SECONDARY OPTION NICKNAME		
	M		O		O		O		
OPER	/	1-32	/	5-36	/	1-23	/	1-23	//

No	Designator	Field Desc	Concept/Explanation/Examples
1	**OPERATION CODEWORD** 1A OPERATION CODEWORD		ENTER THE ASSIGNED OPERATION NAME OR NICKNAME AS ESTABLISHED BY THE APPROPRIATE AUTHORITY, FOR EXAMPLE: "DENY FLIGHT". See table **1020/1** which is an instructive entry
2	**PLAN ORIGINATOR AND NUMBER** 2A PLAN ORIGINATOR AND NUMBER		ENTER THE OPERATION PLAN ORIGINATOR AND NUMBER (NOT THE MESSAGE ORIGINATOR - SEE NOTE 2). FOR EXAMPLE: "SACEUR 106". See table **2404** which is a composite
3	**OPTION NICKNAME** 3A OPTION NICKNAME		ENTER THE NICKNAME OF THE PRIMARY OPTION WITHIN THE OPERATION PLAN, FOR EXAMPLE: "PAPER WASTE". See table **1232/1** which is an instructive entry

No	Designator	Field Desc	Concept/Explanation/Examples
4	**SECONDARY OPTION NICKNAME**		
	4A SECONDARY OPTION NICKNAME		ENTER THE NICKNAME OF THE SECONDARY OPTION WITHIN THE OPERATION PLAN, FOR EXAMPLE: "ORANGE". See table **1232/2** which is an instructive entry

Notes: none

Related Documents: none

Examples:

```
OPER/DENY FLIGHT//
OPER/DENY FLIGHT/SACEUR 106/PAPER WASTE/ORANGE//
OPER/RUBICON//
```

Specific Requirements:: none

PERIOD

Set identifier (Name): PERIOD (PERIOD OF TIME)

	START DAY-TIME		STOP DAY-TIME		QUALIFIED STOP TIME		
	M		M		C		
PERIOD	/	7-15	/	3-15	/	7-15	//

No	Designator		Field Desc	Concept/Explanation/ Examples
1	**START DAY-TIME**			**SPECIFY THE START DAY-TIME-GROUP USING ONE OF THE FOLLOWING:**
	1A	DTG OF START		ENTER THE START DTG, FOR EXAMPLE: "221545ZMAY2004". See table **2033** which is a composite
	1B	DATE-TIME GROUP OF START, VERIFIED		ENTER THE START DTG VERIFIED, FOR EXAMPLE: "120845Z0MAY2008". See table **2034** which is a composite
	1C	DAY-TIME AND MONTH OF START		ENTER THE START DAY-TIME AND MONTH, FOR EXAMPLE "010900ZMAY". See table **2030** which is a composite
	1D	DAY-TIME START		ENTER THE START DAY-TIME, FOR EXAMPLE "010800Z". See table **2000** which is a composite

No	Designator		Field Desc	Concept/Explanation/ Examples
2	**STOP DAY-TIME**			**SPECIFY THE STOP DAY-TIME-GROUP USING ONE OF THE FOLLOWING:**
	2A	DTG OF STOP		ENTER THE STOP DTG, FOR EXAMPLE: "130800ZMAY2004". See table **2033** which is a composite
	2B	DATE-TIME GROUP OF STOP, VERIFIED		ENTER THE STOP DTG VERIFIED, FOR EXAMPLE "010800Z9MAY2004". See table **2034** which is a composite
	2C	DAY-TIME AND MONTH OF STOP		ENTER THE STOP DAY-TIME AND MONTH, FOR EXAMPLE "010900ZMAY". See table **2030** which is a composite
	2D	STOP TIME QUALIFIER		ENTER THE STOP TIME QUALIFIER CODE, FOR EXAMPLE: "UFN". See table **1220/8** which contains a list of data items and associated data codes
	2E	DAY-TIME STOP		ENTER THE STOP DAY-TIME, FOR EXAMPLE "010800Z". See table **2000** which is a composite

No	Designator		Field Desc	Concept/Explanation/ Examples
3	**QUALIFIED STOP TIME**			**IF REQUIRED, SPECIFY THE QUALIFIED STOP TIME IN USING ONE OF THE FOLLOWING:**
	3A	DTG		ENTER THE DTG, FOR EXAMPLE: "201050ZMAY2004". See table **2033** which is a composite
	3B	DTG, VERIFIED		ENTER THE DTG VERIFIED, FOR EXAMPLE "010800Z9MAY2004". See table **2034** which is a composite
	3C	DAY-TIME AND MONTH		ENTER THE DAY-TIME AND MONTH, FOR EXAMPLE "100930ZMAY". See table **2030** which is a composite
	3D	DAY-TIME		ENTER THE DAY-TIME, FOR EXAMPLE "101230Z". See table **2000** which is a composite

Notes: none

Related Documents: none

Examples: `PERIOD/221545ZSEP2006/011200ZOCT2006//`
`PERIOD/221545ZSEP2006/NLT/011200ZOCT2006//`

Specific Requirements:: FIELD 3 IN SET ^ (PERIOD) IS REQUIRED IF FIELD 2 IN SET ^ (PERIOD) EQUALS "AFTER" OR "ASOF" OR "ASAPAFT" OR "ASAPNLT" OR "BEFORE" OR "NET" OR "NLT", OTHERWISE IT IS PROHIBITED.

POCDATA

Set identifier (Name): POCDATA (POINT OF CONTACT)

	RANK OR POSITION		CONTACT NAME		UNIT IDENTIFIER		NON-SECURE TELEPHONE		
	M		M		M		M		
POCDATA	/	1-16	/	1-20	/	1-20	/	1-60	//
							REPEATABLE		

No	Designator	Field Desc	Concept/Explanation/ Examples
1	**RANK OR POSITION**		
	1A RANK OR POSITION		ENTER THE ABREVIATION FOR THE RANK OR POSITION OF THE POINT OF CONTACT, FOR EXAMPLE: "LT-COL". See table **1046/2** which is an instructive entry
2	**CONTACT NAME**		
	2A CONTACT NAME		ENTER THE NAME OF THE POINT OF CONTACT, FOR EXAMPLE: "WYLDE". See table **1022/7** which is an instructive entry
3	**UNIT IDENTIFIER**		
	3A UNIT IDENTIFIER		ENTER THE POINT OF CONTACT'S UNIT DESIGNATION, FOR EXAMPLE: "321 EOD COY". See table **1028/1** which is an instructive entry

No	Designator		Field Desc	Concept/Explanation/ Examples
4	**NON-SECURE TELEPHONE**			
	4A	NON-SECURE TELEPHONE	TEL	ENTER "TEL:" FOLLOWED BY THE NON-SECURE TELEPHONE NUMBER, FOR EXAMPLE: "TEL:12345678910". See table **1361/3** which is an instructive entry
	4B	SECURE TELEPHONE NUMBER	SEC	ENTER "SEC:" FOLLOWED BY THE SECURE TELEPHONE NUMBER, FOR EXAMPLE: "SEC:12345678910". See table **1361/4** which is an instructive entry
	4C	E-MAIL ADDRESS	EMAIL	ENTER "EMAIL:" FOLLOWED BY THE EMAIL ADDRESS, FOR EXAMPLE: "EMAIL: ASMITH(A)MOD.UK" . See table **1614/6** which is an instructive entry
	4D	FAX NUMBER	FAX	ENTER "FAX:" FOLLOWED BY THE FAX NUMBER, FOR EXAMPLE: "FAX:12345678910". See table **1361/10** which is an instructive entry

Notes: none

Related Documents: none

Examples: `POCDATA/LT-COL/WYLDE/321 EOD COY/TEL:12345678910//`

Specific Requirements:: none

REF

Set identifier (Name): REF (REFERENCE)

	SERIAL LETTER		COMMUNICATION TYPE		ORIGINATOR		DATE AND TIME OF REFERENCE		REFERENCE SERIAL NUMBER		SPECIAL NOTATION	
	M		M		M		M		O		O	
REF	/	1-1	/	1-32	/	1-30	/	6-15	/	1-10	/	5-5

	SIC OR FILE NUMBER		
	O		
REF	/	1-10	//
	REPEATABLE		

No	Designator		Field Desc	Concept/Explanation/ Examples
1	**SERIAL LETTER**			
	1A	SERIAL LETTER		ENTER THE ALPHABETIC CHARACTER SEQUENTIALLY ASSIGNED BY THE MESSAGE DRAFTER, FOR EXAMPLE: "A". See table **1102/3** which is an alphanumeric range
2	**COMMUNICATION TYPE**			**SPECIFY THE COMMUNICATION S TYPE USING ONE OF THE FOLLOWING:**
	2A	MESSAGE TEXT FORMAT IDENTIFIER		ENTER THE MESSAGE TEXT FORMAT (MTF) BEING REFERENCED, FOR EXAMPLE: "OPGEN". See table **1018/2** which is an instructive entry
	2B	COMMUNICATION TYPE	TYPE	ENTER "TYPE:" FOLLOWED BY THE COMMUNICATION TYPE IF OTHER THAN AN MTF, FOR EXAMPLE: "TYPE:LTR". See table **1153/1** which contains a list of data items and associated data codes

No	Designator	Field Desc	Concept/Explanation/ Examples
3	**ORIGINATOR**		
	3A ORIGINATOR		ENTER THE ORIGINATOR OF THE MESSAGE, LETTER, OR DOCUMENT REFERENCED, FOR EXAMPLE: "SHAPE". See table **1029/1** which is an instructive entry

No	Designator		Field Desc	Concept/Explanation/ Examples
4	**DATE AND TIME OF REFERENCE**			**SPECIFY THE DATE-TIME OF THE REFERENCE USING ONE OF THE FOLLOWING:**
	4A	DTG OF REFERENCE, 4 DIGIT YR	DTG	ENTER "DTG:" FOLLOWED BY THE DAY-TIME GROUP OF REFERENCE, FOR EXAMPLE: "DTG:150830ZJAN2002". See table **2033** which is a composite
	4B	DAY-TIME OF REFERENCE		ENTER THE DAY-TIME OF REFERENCE, FOR EXAMPLE: "150830Z". See table **2000** which is a composite
	4C	DAY-TIME OF REFERENCE, VERIFIED		ENTER THE VERIFIED DAY-TIME OF REFERENCE, FOR EXAMPLE: "150830Z7". See table **2013** which is a composite
	4D	DAY-TIME AND MONTH OF REFERENCE		ENTER THE DAY-TIME AND MONTH OF REFERENCE, FOR EXAMPLE: "150830ZJAN". See table **2030** which is a composite
	4E	DATE-TIME MONTH OF REFERENCE, VERIFIED		ENTER THE VERIFIED MONTH DATE-TIME OF REFERENCE, FOR EXAMPLE: "150830Z7JAN". See table **2032** which is a composite
	4F	DAY-TIME GROUP OF REFERENCE		ENTER THE DATE-TIME GROUP OF REFERENCE, FOR EXAMPLE: "150830ZJAN1996". See table **2197** which is a composite
	4G	DTG OF REFERENCE, VERIFIED, 4 YR		ENTER THE VERIFIED DATE-TIME GROUP OF REFERENCE, FOR EXAMPLE: "150830Z7JAN1996". See table **2034** which is a composite

No	Designator		Field Desc	Concept/Explanation/ Examples
	4H	DATE OF REFERENCE, DDMMMYYYY		ENTER THE DATE OF REFERENCE, DAY-ALPHAMONTH-YEAR, FOR EXAMPLE: "15JAN1994". See table **2001** which is a composite
	4I	DATE OF REFERENCE, DDMMYYYY	DMY	ENTER "DMY:" FOLLOWED BY THE DATE OF REFERENCE, FOR EXAMPLE: "DMY:15011994". See table **2052** which is a composite
	4J	DATE OF REFERENCE, YYYYMMDD	YMD	ENTER "YMD:" FOLLOWED BY THE DATE OF REFERENCE, FOR EXAMPLE: "YMD:19940115". See table **2053** which is a composite
5	**REFERENCE SERIAL NUMBER**			
	5A	REFERENCE SERIAL NUMBER		ENTER THE MESSAGE SERIAL NUMBER, FOR EXAMPLE: "100" OR DOCUMENT SERIAL NUMBER, FOR EXAMPLE: "AIR 051". See table **1012/66** which is an instructive entry
6	**SPECIAL NOTATION**			
	6A	SPECIAL NOTATION		ENTER THE SPECIAL NOTATION WHICH APPLIES TO THE REFERENCED MESSAGE, FOR EXAMPLE: "NOTAL". See table **1131/1** which contains a list of data items and associated data codes

No	Designator		Field Desc	Concept/Explanation/ Examples
7	**SIC OR FILE NUMBER**			**SPECIFY THE SIC OR FILE NUMBER USING ONE OF THE FOLLOWING, REPEATING AS NECESSARY:**
	7A	SIC		ENTER THE SIC, FOR EXAMPLE: "RCA". See table **1017/2** which is an instructive entry
	7B	FILING NUMBER	FN	ENTER "FN:" FOLLOWED BY THE FILE NUMBER LISTED ON THE REFERENCE DOCUMENT, FOR EXAMPLE: "FN:4503B". See table **1012/49** which is an instructive entry

Notes: SPECIFIES IDENTIFYING DETAILS REGARDING A DOCUMENT, IMAGE OR OTHER INFORMATION EXCHANGE MEDIA THAT IS APPLICABLE TO THE CONTENT OF THIS MESSAGE.

Related Documents: none

Examples:

```
REF/A/LTR/SHAPE/28072006/AIR 051//
REF/B/OPGEN/SACLANT/150830ZJAN2006/100/NOTAL/RCA/RDU
//
```

Specific Requirements:: none

RMKS

Set identifier (Name): RMKS (REMARKS)

	FREE TEXT M		
RMKS	/	1-Unbounded	//

No	Designator	Field Desc	Concept/Explanation/ Examples
1	**FREE TEXT**		
	1A FREE TEXT		ENTER IN FREE TEXT INFORMATION THAT PRETAINS TO THE MESSAGE AS A WHOLE. See table **1006/1** which is an instructive entry

Notes: none

Related Documents: none

Examples:

```
RMKS/ENSURE ONWARD DISEMINATION OF THIS MESSAGE TO
ALL COMMANDERS IN
THE FIELD//
```

Specific Requirements:: none

SYSTEM

Set identifier (Name): SYSTEM (SYSTEM NAME)

	IP SYSTEM M		
SYSTEM	/	1-32	//

No	Designator	Field Desc	Concept/Explanation/ Examples
1	**IP SYSTEM** 1A IP BASED SYSTEM		**Specifies the name of the System that the remainder of the segment refers to.** Enter the name of the system, for example: "CENTRIXS". See table **1135/999** which is an instructive entry

Notes: none

Related Documents: none

Examples: SYSTEM/CENTRIXS//

Specific Requirements:: none

UNITIP

Set identifier (Name): UNITIP (UNIT INTERNET PROTOCOL SETTINGS)

	UNIT NAME		IP CRYPTO DEVICE		IP KEYMAT		IP ADDRESS OF RED CRYPTO		IP ADDRESS OF BLACK CRYPTO		SYSTEM IP ADDRESS	
	M		M		M		M		M		M	
UNITIP	/	1-38	/	1-16	/	8-10	/	7-15	/	7-15	/	7-15

	LOCAL BEARER ADDRESS		
	M		
UNITIP	/	1-3	//
	REPEATABLE 2 TIMES		

No	Designator	Field Desc	Concept/Explanation/ Examples
1	**UNIT NAME**		**Specifies the name of the unit that the rest of the segment refers to.**
	1A UNIT NAME		Enter the unit name. for example: "HMS DARING". See table **1022/48** which is an instructive entry
2	**IP CRYPTO DEVICE**		**Specifies the crypto device fitted to the unit.**
	2A TYPE OF CRYPTOGRAPHIC EQUIPMENT		Enter the name of the crypto device, for example: "XYZ123". See table **1135/18** which is an instructive entry
3	**IP KEYMAT**		**Specifies the IP KEYMAT that is used by the crypto device.**
	3A SHIP-SHORE KEYMAT		Enter the KEYMAT to be used by the unit, for example: "ABCD4321". See table **1078/6** which is an instructive entry

No	Designator	Field Desc	Concept/Explanation/ Examples
4	**IP ADDRESS OF RED CRYPTO**		**Specifies the IP Address of Red Crypto assigned to the unit.**
	4A IPV4 ADDRESS		Enter and IPv4 Address, for example: "168.123.012.3". See table **6004** which is a composite
5	**IP ADDRESS OF BLACK CRYPTO**		**Specifies the IP Address of Black Crypto assigned to the unit.**
	5A IPV4 ADDRESS		Enter and IPv4 Address, for example: "178.123.012.3". See table **6004** which is a composite
6	**SYSTEM IP ADDRESS**		**Specifies the IP Address assigned to the units router.**
	6A IPV4 ADDRESS		Enter and IPv4 Address, for example: "188.123.012.3". See table **6004** which is a composite

No	Designator		Field Desc	Concept/Explanation/ Examples
7	**LOCAL BEARER ADDRESS**			**Specifies the local bearer address. Where more than one local bearer address can be applied, this field may be repeated.**
	7A	NODE NUMBER	NODE	Enter "NODE:" followed by the local bearer address as a node number, for example: "NODE:5". See table **1012/701** which is a range [1 through 99]
	7B	CONTROLLER NUMBER	CONT	Enter "CONT:" followed by the local bearer address as a Controller Number, for example: "CONT:9". See table **1012/702** which is a range [1 through 256]
	7C	MODEM NUMBER	MODEM	Enter "MODEM:" followed by the local bearer address as a Modem Number, for example: "MODEM:123". See table **1012/703** which is a range [1 through 999]
	7D	INTERNET PROTOCOL (IP) ADDRESS OCTET		Enter by the local bearer address as a IPv4 Address, for example: "168.3.56.12". See table **1012/700** which is a range [0 through 255]

Notes: none

Related Documents: none

Examples: `UNITIP/HMS DARING/XYZ123/ABCD4321/168.123.012.3/178.123.012.3 /188.123.012.3/CONT:9//`

Specific Requirements:: none

UNITSVC

Set identifier (Name): UNITSVC (UNIT SERVICES)

	OPERATIONAL SERVICE		SERVICE IP ADDRESS		PORT NUMBER		Remarks		
	M		M		M		O		
UNITSVC	/	1-32	/	7-15	/	1-5	/	1-68	//

No	Designator		Field Desc	Concept/Explanation/ Examples
1	**OPERATIONAL SERVICE**			**Specifies the operational service that the following settings apply to.**
	1A	NETWORK SERVICE NAME		Enter the name of the service, for example: "CHAT". See table **1022/802** which is an instructive entry
2	**SERVICE IP ADDRESS**			**The IP Address of the network service.**
	2A	IPV4 ADDRESS		Enter the IP v4 Address of the service, for example: "168.1.123.45". See table **6004** which is a composite
3	**PORT NUMBER**			**The port number assigned to the service.**
	3A	PORT NUMBER		Enter the port number, for example: "8082". See table **1012/704** which is a range [0 through 65535]
4	**Remarks**			**Add any service specific remarks.**
	4A	REMARKS		Enter remarks, for example: "BLUE RED ONLY". See table **1357/28** which is an instructive entry

Notes: none

Related Documents: none

Examples: `UNITSVC/CHAT/168.1.123.45/8082/BLUE RED ONLY//`

Specific Requirements:: none

Elemental Tables

Table 1000/1 - DAY (2-2)

Related Documents: None

Explanation: None

DAY	Range - Integer (2-2)		Explanation
	MIN Value	MAX Value	None
	01	31	

Table 1001/1 - HOUR (TIME) (2-2)

Related Documents: None

Explanation: HOUR IS EXPRESSED IN 00-23.

HOUR (TIME)	Range - Integer (2-2)		Explanation
	MIN Value	MAX Value	None
	00	23	

Table 1002/1 - MINUTE (TIME) (2-2)

Related Documents: None

Explanation: None

MINUTE (TIME)	Range - Integer (2-2)		Explanation
	MIN Value	MAX Value	None
	00	59	

Table 1003/1 - TIME ZONE (1-1)

Related Documents: None

Explanation: None

TIME ZONE (Data Item)	Data Code	Explanation
UNIVERSAL TIME COORDINATE (UTC)	Z	None
UTC PLUS 1 HOUR	A	None
UTC PLUS 2 HOURS	B	None
UTC PLUS 3 HOURS	C	None
UTC PLUS 4 HOURS	D	None
UTC PLUS 5 HOURS	E	None
UTC PLUS 6 HOURS	F	None
UTC PLUS 7 HOURS	G	None
UTC PLUS 8 HOURS	H	None
UTC PLUS 9 HOURS	I	None
UTC PLUS 10 HOURS	K	None
UTC PLUS 11 HOURS	L	None
UTC PLUS 12 HOURS	M	None
UTC MINUS 1 HOUR	N	None
UTC MINUS 2 HOURS	O	None
UTC MINUS 3 HOURS	P	None
UTC MINUS 4 HOURS	Q	None
UTC MINUS 5 HOURS	R	None
UTC MINUS 6 HOURS	S	None
UTC MINUS 7 HOURS	T	None
UTC MINUS 8 HOURS	U	None
UTC MINUS 9 HOURS	V	None
UTC MINUS 10 HOURS	W	None
UTC MINUS 11 HOURS	X	None
UTC MINUS 12 HOURS	Y	None

Table 1004/1 - MONTH NAME (3-3)

Related Documents: None

Explanation: None

MONTH NAME (Data Item)	Data Code	Explanation
JANUARY	JAN	None
FEBRUARY	FEB	None
MARCH	MAR	None
APRIL	APR	None
MAY	MAY	None
JUNE	JUN	None
JULY	JUL	None
AUGUST	AUG	None
SEPTEMBER	SEP	None
OCTOBER	OCT	None
NOVEMBER	NOV	None
DECEMBER	DEC	None

Table 1004/9 - MONTH (2-2)

Related Documents: None

Explanation: ONE OF THE TWELVE PARTS INTO WHICH A YEAR IS DIVIDED AS DEFINED BY THE GREGORIAN CALENDAR.

MONTH (Data Item)	Data Code	Explanation
JANUARY	01	None
FEBRUARY	02	None
MARCH	03	None
APRIL	04	None
MAY	05	None
JUNE	06	None
JULY	07	None
AUGUST	08	None
SEPTEMBER	09	None
OCTOBER	10	None
NOVEMBER	11	None
DECEMBER	12	None

Table 1005/7 - YEAR (4-4)

Related Documents: None

Explanation: None

YEAR	Range - Integer (4-4)		Explanation
	MIN Value	MAX Value	None
	0001	9999	

Table 1006/1 - FREE TEXT (1-Unbounded)

Related Documents: None

Explanation: AN UNFORMATTED FREE TEXT FIELD CONTAINING AN UNLIMITED NUMBER OF CHARACTERS USED IN THE FREE SET AMPN, GENTEXT, NARR AND RMKS. ALL CHARACTER TYPES ARE ALLOWED EXCEPT DOUBLE SLANTS (//).

FREE TEXT	Instructive - Allowable Entries (1-Unbounded)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1008/2 - UNIT OF ELECTROMAGNETIC EMISSION MEASUREMENT (2-3)

Related Documents: None

Explanation: None

UNIT OF ELECTROMAGNETIC EMISSION MEASUREMENT (Data Item)	Data Code	Explanation
GIGAHERTZ	GHZ	None
HERTZ	HZ	None
KILOHERTZ	KHZ	None
MEGAHERTZ	MHZ	None

Table 1008/113 - UNIT OF DATA RATE MEASUREMENT (3-4)

Related Documents: None

Explanation: None

UNIT OF DATA RATE MEASUREMENT (Data Item)	Data Code	Explanation
BITS, BITS PER SECOND	BPS	None
BITS, GIGABITS PER SECOND	GBPS	None
BITS, KILOBITS PER SECOND	KBPS	None
BITS, MEGABITS PER SECOND	MBPS	None

Table 1009/1 - TEXT INDICATOR (1-61)

Related Documents: None

Explanation: AN INDICATION OF THE SUBJECT MATTER ADDRESSED IN A GENERAL TEXT (GENTEXT) SET.

TEXT INDICATOR	Instructive - Allowable Entries (1-61)	Explanation
Alphabetic upper case, Blank, Numeric, Special		ENTER THE NAME WHICH INDICATES THE SUBJECT MATTER TO BE DISCUSSED.

Table 1012/7 - MESSAGE SERIAL NUMBER (1-13)

Related Documents: None
Explanation: SEE ACP 121.

MESSAGE SERIAL NUMBER	Range - Integer (1-13)		Explanation
	MIN Value	MAX Value	AN ALPHANUMERIC OR LITERAL SYMBOL IDENTIFYING A PARTICULAR ITEM OF A SEQUENCE OR SERIES.
	0	9999999999999	

Table 1012/29 - SERIAL NUMBER OF QUALIFIER (1-3)

Related Documents: None
Explanation: None

SERIAL NUMBER OF QUALIFIER	Range - Integer (1-3)		Explanation
	MIN Value	MAX Value	None
	1	999	

Table 1012/49 - FILING NUMBER (1-10)

Related Documents: None
Explanation: None

FILING NUMBER	Instructive - Allowable Entries (1-10)	Explanation
Alphabetic upper case, Blank, Numeric, Special		AN ALPHANUMERIC OR LITERAL SYMBOL IDENTIFYING A PARTICULAR ITEM OF A SEQUENCE OR SERIES.

Table 1012/66 - REFERENCE SERIAL NUMBER (1-10)

Related Documents: None
Explanation: None

REFERENCE SERIAL NUMBER	Instructive - Allowable Entries (1-10)	Explanation
Alphabetic upper case, Blank, Numeric, Special		AN ALPHANUMERIC OR LITERAL SYMBOL IDENTIFYING A PARTICULAR ITEM OF A SEQUENCE OR SERIES.

Table 1012/146 - PLAN NUMBER (1-15)

Related Documents: None
Explanation: None

PLAN NUMBER	Instructive - Allowable Entries (1-15)	Explanation
Alphabetic upper case, Numeric, Special		AN ALPHANUMERIC OR LITERAL SYMBOL IDENTIFYING A PARTICULAR ITEM OF A SEQUENCE OR SERIES.

Table 1012/700 - INTERNET PROTOCOL (IP) ADDRESS OCTET (1-3)

Related Documents: None

Explanation: INTERNET PROTOCOL (IP) ADDRESS OCTET

INTERNET PROTOCOL (IP) ADDRESS OCTET	Range - Integer (1-3)		Explanation
	MIN Value	MAX Value	None
	0	255	

Table 1012/701 - NODE NUMBER (1-2)

Related Documents: None

Explanation: The number of a node.

NODE NUMBER	Range - Integer (1-2)		Explanation
	MIN Value	MAX Value	None
	1	99	

Table 1012/702 - CONTROLLER NUMBER (1-3)

Related Documents: None

Explanation: The number assigned to a controller.

CONTROLLER NUMBER	Range - Integer (1-3)		Explanation
	MIN Value	MAX Value	None
	1	256	

Table 1012/703 - MODEM NUMBER (1-3)

Related Documents: None

Explanation: The number assigned to a modem.

MODEM NUMBER	Range - Integer (1-3)		Explanation
	MIN Value	MAX Value	None
	1	999	

Table 1012/704 - PORT NUMBER (1-5)

Related Documents: None

Explanation: a port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system.

PORT NUMBER	Range - Integer (1-5)		Explanation
	MIN Value	MAX Value	None
	0	65535	

Table 1017/2 - SIC (3-3)

Related Documents: None

Explanation: None

SIC	Instructive - Allowable Entries (3-3)	Explanation
Alphabetic upper case, Numeric		None

Table 1018/11 - EXERCISE ADDITIONAL IDENTIFIER (4-16)

Related Documents: None

Explanation: None

EXERCISE ADDITIONAL IDENTIFIER (Data Item)	Data Code	Explanation
MSG BETWEEN "BLUE" PLAYERS	BLUE	None
MSG ADDRESSED TO PLAYERS TO CONTROL THE EXERCISE	CONTROL	None
MSG FOR DISTAFF OR DICONSTAFF ONLY	DISTAFF	None
MSG FOR TEST OR PRACTICE NOT RELATED TO THE EXERCISE	DRILL	None
MSG NOT PART OF PLAY BUT AFFECTING THE EXERCISE	NO PLAY	None
MSG INTERCEPTION NOT FOR USE IN DIRECTION FINDING	NODUF	None
MSG BETWEEN "ORANGE" PLAYERS	ORANGE	None
MSG ORIGINATED BY A COMMANDER ASSIGNED A "PURPLE" ROLE	PURPLE	None
MSG ORIGINATED BY AN UMPIRE	UMPIRE	None
MSG ADDRESSED TO UMPIRES ONLY	UMPIRE EYES ONLY	None

Table 1018/2 - MESSAGE TEXT FORMAT IDENTIFIER (1-32)

Related Documents: None
Explanation: None

MESSAGE TEXT FORMAT IDENTIFIER	Instructive - Allowable Entries (1-32)	Explanation
Alphabetic upper case, Blank		None

Table 1018/11 - EXERCISE ADDITIONAL IDENTIFIER (4-16)

Related Documents: None
Explanation: None

EXERCISE ADDITIONAL IDENTIFIER (Data Item)	Data Code	Explanation
MSG BETWEEN "BLUE" PLAYERS	BLUE	None
MSG ADDRESSED TO PLAYERS TO CONTROL THE EXERCISE	CONTROL	None
MSG FOR DISTAFF OR DICONSTAFF ONLY	DISTAFF	None
MSG FOR TEST OR PRACTICE NOT RELATED TO THE EXERCISE	DRILL	None
MSG NOT PART OF PLAY BUT AFFECTING THE EXERCISE	NO PLAY	None
MSG INTERCEPTION NOT FOR USE IN DIRECTION FINDING	NODUF	None
MSG BETWEEN "ORANGE" PLAYERS	ORANGE	None
MSG ORIGINATED BY A COMMANDER ASSIGNED A "PURPLE" ROLE	PURPLE	None
MSG ORIGINATED BY AN UMPIRE	UMPIRE	None
MSG ADDRESSED TO UMPIRES ONLY	UMPIRE EYES ONLY	None

Table 1020/1 - OPERATION CODEWORD (1-32)

Related Documents: None

Explanation: None

OPERATION CODEWORD	Instructive - Allowable Entries (1-32)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1021/1 - EXERCISE NICKNAME (1-56)

Related Documents: None

Explanation: None

EXERCISE NICKNAME	Instructive - Allowable Entries (1-56)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1022/7 - CONTACT NAME (1-20)

Related Documents: None

Explanation: THE NAME OF THE PERSON TO BE CONTACTED.

CONTACT NAME	Instructive - Allowable Entries (1-20)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1022/48 - UNIT NAME (1-38)

Related Documents: None

Explanation: None

UNIT NAME	Instructive - Allowable Entries (1-38)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1022/801 - TIME SOURCE (1-64)

Related Documents: None

Explanation: The source of the time synchronization for the bearer.

TIME SOURCE	Instructive - Allowable Entries (1-64)	Explanation
Alphabetic lower case, Alphabetic upper case, Blank, Numeric, Special		None

Table 1022/802 - NETWORK SERVICE NAME (1-32)

Related Documents: None

Explanation: The common name assigned to a network service.

NETWORK SERVICE NAME	Instructive - Allowable Entries (1-32)	Explanation
Alphabetic lower case, Alphabetic upper case, Blank, Extended Special, Numeric, Special		None

Table 1023/13 - CONTEXT QUANTITY, 0-9 (1-1)

Related Documents: None

Explanation: None

CONTEXT QUANTITY, 0-9	Range - Integer (1-1)		Explanation
	MIN Value	MAX Value	None
	0	9	

Table 1023/22 - CONTEXT QUANTITY, DECIMAL PT PERMITTED, 11 CHAR MAX (1-22)

Related Documents: None

Explanation: None

CONTEXT QUANTITY, DECIMAL PT PERMITTED, 11 CHAR MAX		Range - Decimal (1-22)		Explanation
MIN Places	MAX Places	MIN Value	MAX Value	THE VALUES ARE THE INTEGERS 0 THROUGH 99999999999, AND DECIMAL POINT VALUES. THE DECIMAL POINT VALUES CONSIST OF ALL THE VALUES IN THE RANGE OF .0000000001 THROUGH 999999999.9, INCREMENTED BY: .0000000001 IN THE RANGE OF .0000000001 THROUGH .9999999999: .000000001 IN THE RANGE OF .0000000001 THROUGH 9.999999999; .00000001 IN THE RANGE OF .0000000001 THROUGH 99.99999999; .0000001 IN THE RANGE OF .0000000001 THROUGH 999.9999999; .000001 IN THE RANGE OF .0000000001 THROUGH 9999.999999; .00001 IN THE RANGE OF .0000000001 THROUGH 99999.99999; .0001 IN THE RANGE OF .0000000001 THROUGH 999999.9999; .001 IN THE RANGE OF .0000000001 THROUGH 9999999.999; .01 IN THE RANGE OF .000000001 THROUGH 99999999.99; .1 IN THE RANGE OF .0000000001 THROUGH 999999999.9.
0	10	0	99999999999.0000000000	

Table 1023/28 - CONTEXT QUANTITY, DECIMAL PT PERMITTED, 6 CHAR MAX (1-12)

Related Documents: None

Explanation: None

CONTEXT QUANTITY, DECIMAL PT PERMITTED, 6 CHAR MAX		Range - Decimal (1-12)		Explanation
MIN Places	MAX Places	MIN Value	MAX Value	THE VALUES ARE THE

CONTEXT QUANTITY, DECIMAL PT PERMITTED, 6 CHAR MAX		Range - Decimal (1-12)		Explanation
0	5	0	999999.00000	INTEGERS 0 THROUGH 999999, AND DECIMAL POINT VALUES. THE DECIMAL POINT VALUES CONSIST OF ALL THE VALUES IN THE RANGE OF .00001 THROUGH 9999.9, INCREMENTED BY: .00001 IN THE RANGE OF .00001 THROUGH .99999; .0001 IN THE RANGE OF .00001 THROUGH 9.9999; .001 IN THE RANGE OF .00001 THROUGH 99.999; .01 IN THE RANGE OF .00001 THROUGH 999.99; .1 IN THE RANGE OF .00001 THROUGH 9999.9.

Table 1025/3 - DECIMAL POINT (1-1)

Related Documents: None
Explanation: None

DECIMAL POINT (Data Item)	Data Code	Explanation
DECIMAL POINT	.	None

Table 1025/4 - BLANK SPACE CHARACTER (1-1)

Related Documents: None
Explanation: None

BLANK SPACE CHARACTER	Instructive - Allowable Entries (1-1)	Explanation
Blank		BLANK OR SPACE

Table 1028/1 - UNIT IDENTIFIER (1-20)

Related Documents: None

Explanation: None

UNIT IDENTIFIER	Instructive - Allowable Entries (1-20)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1029/1 - ORIGINATOR (1-30)

Related Documents: None
Explanation: None

ORIGINATOR	Instructive - Allowable Entries (1-30)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1029/2 - PLAN ORIGINATOR (3-20)

Related Documents: None
Explanation: None

PLAN ORIGINATOR	Instructive - Allowable Entries (3-20)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1046/2 - RANK OR POSITION (1-16)

Related Documents: None

Explanation: THE RANK OR POSITION OF THE SUBJECT HUMAN BEING.

RANK OR POSITION	Instructive - Allowable Entries (1-16)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1078/4 - CRYPTO KEYING MATERIAL (8-10)

Related Documents: None

Explanation: CRYPTO KEYING MATERIAL DESIGNATION ACCORDING TO AMSG-600.

CRYPTO KEYING MATERIAL	Instructive - Allowable Entries (8-10)	Explanation
Alphabetic upper case, Numeric, Special		None

Table 1078/6 - SHIP-SHORE KEYMAT (8-10)

Related Documents: None

Explanation: None

SHIP-SHORE KEYMAT	Instructive - Allowable Entries (8-10)	Explanation
Alphabetic upper case, Numeric, Special		None

Table 1102/3 - SERIAL LETTER (1-1)

Related Documents: None

Explanation: AN ALPHABETIC CHARACTER IDENTIFYING AN INDIVIDUAL COMMUNICATION.

SERIAL LETTER		**Range - Alphanumeric (1-1)**		**Explanation**
First Value	Second Value	Last Value	Omit	None
A	B	Z		

Table 1130/3 - QUALIFIER (3-3)

Related Documents: None

Explanation: A UNIQUE CODE WHICH CAVEATS A MESSAGE STATUS.

QUALIFIER (Data Item)	Data Code	Explanation
AMPLIFYING	AMP	None
BLOCK	BLK	BLOCK TIME PERIODS.
CHANGE	CHG	DIRECTS A SEQUENTIAL CHANGE TO A PREVIOUSLY SENT MESSAGE.
DEVIATION	DEV	None
FINAL	FIN	None
FOLLOW-UP	FUP	None
INITIAL	INI	None
PERMANENT	PER	None
REQUEST	REQ	None
UPDATE	UPD	None

Table 1130/3 - QUALIFIER (3-3)

Related Documents: None

Explanation: A UNIQUE CODE WHICH CAVEATS A MESSAGE STATUS.

QUALIFIER (Data Item)	Data Code	Explanation
AMPLIFYING	AMP	None
BLOCK	BLK	BLOCK TIME PERIODS.
CHANGE	CHG	DIRECTS A SEQUENTIAL CHANGE TO A PREVIOUSLY SENT MESSAGE.
DEVIATION	DEV	None
FINAL	FIN	None
FOLLOW-UP	FUP	None
INITIAL	INI	None
PERMANENT	PER	None
REQUEST	REQ	None
UPDATE	UPD	None

Table 1131/1 - SPECIAL NOTATION (5-5)

Related Documents: None

Explanation: None

SPECIAL NOTATION (Data Item)	Data Code	Explanation
PASSED SEPARATELY	PASEP	BEING PASSED SEPARATELY.
NOT TO ALL	NOTAL	NOT TO ALL NOR NEEDED BY ALL ADDRESSEES.

Table 1135/18 - TYPE OF CRYPTOGRAPHIC EQUIPMENT (1-16)

Related Documents: None

Explanation: THE TYPE OF COMMUNICATIONS ENCRYPTION EQUIPMENT HELD.

TYPE OF CRYPTOGRAPHIC EQUIPMENT	Instructive - Allowable Entries (1-16)	Explanation
Alphabetic upper case, Numeric		None

Table 1135/999 - IP BASED SYSTEM (1-32)

Related Documents: None

Explanation: A system that uses Internet Protocol as its primary method of exchanging data.

IP BASED SYSTEM	Instructive - Allowable Entries (1-32)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1153/1 - COMMUNICATION TYPE (2-3)

Related Documents: None

Explanation: None

COMMUNICATION TYPE (Data Item)	Data Code	Explanation
CONFERENCE	CON	None
DOCUMENT	DOC	None
ELECTRONIC MAIL	EML	None
LETTER/MEMORANDUM	LTR	None
MESSAGE (NOT FORMATTED)	MSG	None
OPERATION ORDER	OPO	None
TELEVISION	TV	None
VIDEO TELECONFERENCE	VTC	None
MEETING	MTG	None

Table 1220/8 - STOP TIME QUALIFIER (3-7)

Related Documents: None

Explanation: None

STOP TIME QUALIFIER (Data Item)	Data Code	Explanation
AFTER	AFTER	None
AS SOON AS POSSIBLE	ASAP	None
AS SOON AS POSSIBLE AFTER	ASAPAFT	None
AS SOON AS POSSIBLE NOT LATER THAN	ASAPNLT	None
AS OF	ASOF	None
BEFORE	BEFORE	None
INDEFINITE	INDEF	None
NOT EARLIER THAN	NET	None
NOT LATER THAN	NLT	None
ON CALL	ONCALL	None
TO BE DETERMINED	TBD	None
UNTIL FURTHER NOTICE	UFN	None
UNKNOWN	UNK	None

Table 1232/1 - OPTION NICKNAME (1-23)

Related Documents: None

Explanation: None

OPTION NICKNAME	Instructive - Allowable Entries (1-23)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1232/2 - SECONDARY OPTION NICKNAME (1-23)

Related Documents: None

Explanation: None

SECONDARY OPTION NICKNAME	Instructive - Allowable Entries (1-23)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1275/900 - Wide Area Network Bearer (2-8)

Related Documents: None

Explanation: None

Wide Area Network Bearer (Data Item)	Data Code	Explanation
SATCOM	SAT	None
UHF SATCOM	U-SAT	None
SHF SATCOM	S-SAT	None
HD SNR	HD SNR	None
Subnet Relay	SNR	None
High Capacity Data Radio	HCDR	None
Enhanced High Capacity Data Radio	E-HCDR	None
Wide Band HF	WBHF	None
Free Space Optics	FSO	None
Third generation mobile telecommunications technology	3G	Complies with International Mobile Telecommunications-2000 (IMT-2000) specifications by the International Telecommunication Union.
Fourth generation of mobile telecommunications technology	4G	Complies with International Mobile Telecommunications Advanced (IMT-Advanced) specification
INMARSAT	INMARSAT	None

Table 1275/901 - Generic Bearer (1-24)

Related Documents: None

Explanation: Allows the MTF drafter to complete an alterantive entry for a Bearer. This allows for beraers that were not known about at the time the IER was developed.

Generic Bearer	Instructive - Allowable Entries (1-24)	Explanation
Alphabetic upper case, Blank, Numeric, Special		Allows the MTF drafter to complete an alterantive entry for a Bearer. This allows for beraers that were not known about at the time the IER was developed.

Table 1357/28 - REMARKS (1-68)

Related Documents: None

Explanation: ENABLES ADDITIONAL TEXT TO BE ATTACHED TO THE FIELDS IT REFERS TO.

REMARKS	Instructive - Allowable Entries (1-68)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1361/3 - NON-SECURE TELEPHONE (3-20)

Related Documents: None

Explanation: THE DESIGNATED NON-SECURE TELEPHONE NUMBER OF AN INDIVIDUAL OR AGENCY TO BE CONTACTED.

NON-SECURE TELEPHONE	Instructive - Allowable Entries (3-20)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1361/4 - SECURE TELEPHONE NUMBER (4-20)

Related Documents: None

Explanation: THE DESIGNATED SECURE TELEPHONE NUMBER OF AN INDIVIDUAL OR AGENCY TO BE CONTACTED.

SECURE TELEPHONE NUMBER	Instructive - Allowable Entries (4-20)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1361/10 - FAX NUMBER (1-23)

Related Documents: None

Explanation: ACTUAL FAX NUMBER.

FAX NUMBER	Instructive - Allowable Entries (1-23)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Table 1614/6 - E-MAIL ADDRESS (1-60)

Related Documents: None

Explanation: None

E-MAIL ADDRESS	Instructive - Allowable Entries (1-60)	Explanation
Alphabetic upper case, Blank, Numeric, Special		None

Composite Tables

Table 2000 - DAY-TIME (7-7)

Related Documents: NONE

Definition: THE DAY OF A MONTH AND TIMEKEEPING IN HOURS AND MINUTES OF A CALENDAR DAY CLOCK SYSTEM AND AN ASSOCIATED TIME ZONE.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)

Table 2001 - DATE, DDMMMYYYY (9-9)

Related Documents: NONE

Definition: A POINT IN TIME EXPRESSED AS DAY(DD), ALPHAMONTH (MMM) AND 4-DIGIT YEAR (YYYY).

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	MONTH NAME	See table **1004/1** which is a coded item (3)
3	YEAR	See table **1005/7** which is a range [0001 through 9999] (4)

Table 2013 - DAY-TIME, VERIFIED (8-8)

Related Documents: NONE

Definition: THE DAY OF THE MONTH AND TIMEKEEPING IN HOURS AND MINUTES OF A CALENDAR DAY, USING THE 24-HOUR CLOCK SYSTEM AND AN ASSOCIATED TIME ZONE, AND A CHECKSUM DIGIT FOR VERIFICATION.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)
5	CONTEXT QUANTITY, 0-9	See table **1023/13** which is a range [0 through 9] (1)

Table 2030 - DAY-TIME AND MONTH (10-10)

Related Documents: NONE

Definition: THE DAY OF A MONTH AND TIMEKEEPING IN HOURS AND MINUTES OF A CALENDAR DAY, USING THE 24-HOUR CLOCK SYSTEM, ASSOCIATED TIME ZONE AND MONTH.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)
5	MONTH NAME	See table **1004/1** which is a coded item (3)

Table 2032 - DATE-TIME MONTH, VERIFIED (11-11)

Related Documents: NONE

Definition: DAY OF THE MONTH, TIMEKEEPING IN HOURS AND MINUTES OF A CALENDAR DAY USING THE 24-HOUR CLOCK SYSTEM AND AN ASSOCIATED TIME ZONE WITH A CHECKSUM DIGIT FOR VERIFICATION WITH MONTH OF THE YEAR.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)
5	CONTEXT QUANTITY, 0-9	See table **1023/13** which is a range [0 through 9] (1)
6	MONTH NAME	See table **1004/1** which is a coded item (3)

Table 2033 - DTG (14-14)

Related Documents: AAP-6

Definition: A DATE-TIME GROUP (DTG) OF SIX DIGITS WITH A TIME ZONE SUFFIX AND THE STANDARDIZED ABBREVIATION FOR THE MONTH AND A 4-DIGIT YEAR. THE FIRST PAIR OF THE SIX DIGITS REPRESENTS THE DAY; THE SECOND PAIR THE HOUR; THE THIRD PAIR THE MINUTES.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)
5	MONTH NAME	See table **1004/1** which is a coded item (3)
6	YEAR	See table **1005/7** which is a range [0001 through 9999] (4)

Table 2034 - DTG, VERIFIED, 4-DIGIT YEAR (15-15)

Related Documents: NONE

Definition: A DATE-TIME GROUP (DTG) OF SIX DIGITS WITH A ZONE TIME SUFFIX, A CHECKSUM DIGIT FOR VERIFICATION, THE STANDARDIZED ABBREVIATION FOR THE MONTH AND A 4-DIGIT YEAR. THE FIRST PAIR OF THE SIX DIGITS REPRESENTS THE DAY; THE SECOND PAIR THE HOUR; THE THIRD PAIR THE MINUTES.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)
4	TIME ZONE	See table **1003/1** which is a coded item (1)
5	CONTEXT QUANTITY, 0-9	See table **1023/13** which is a range [0 through 9] (1)
6	MONTH NAME	See table **1004/1** which is a coded item (3)
7	YEAR	See table **1005/7** which is a range [0001 through 9999] (4)

Table 2052 - DATE, DDMMYYYY (8-8)

Related Documents: NONE

Definition: A POINT IN TIME EXPRESSED AS DAY (DD), MONTH (MM), AND YEAR (YYYY).

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	MONTH	See table **1004/9** which is a coded item (2)
3	YEAR	See table **1005/7** which is a range [0001 through 9999] (4)

Table 2053 - DATE, YYYYMMDD (8-8)

Related Documents: AINTP-3
STANAG 2433

Definition: A GROUP OF 8 DIGITS DEFINING A POINT IN TIME EXPRESSED AS YEAR (YYYY), MONTH (MM) AND DAY (DD).

Seq	Elemental FUD Name	Elemental Use
1	YEAR	See table **1005/7** which is a range [0001 through 9999] (4)
2	MONTH	See table **1004/9** which is a coded item (2)
3	DAY	See table **1000/1** which is a range [01 through 31] (2)

Table 2064 - RADIO FREQUENCY (3-25)

Related Documents: STANAG 6004

Definition: THE CENTER FREQUENCY AT WHICH ELECTROMAGNETIC RADIATION OF ENERGY IS POSSIBLE.

Seq	Elemental FUD Name	Elemental Use
1	CONTEXT QUANTITY, DECIMAL PT PERMITTED, 11 CHAR MAX	See table **1023/22** which is a range [0 through 99999999999.0000000000] (0 to 10 decimal places) (1-22)
2	UNIT OF ELECTROMAGNETIC EMISSION MEASUREMENT	See table **1008/2** which is a coded item (2-3)

Table 2197 - DAY-TIME GROUP (6-6)

Related Documents: STANAG 5620

Definition: DAY AND TIME OF A REPORT OR REFERENCE TO A MISSION OR ACTIVITY.

Seq	Elemental FUD Name	Elemental Use
1	DAY	See table **1000/1** which is a range [01 through 31] (2)
2	HOUR (TIME)	See table **1001/1** which is a range [00 through 23] (2)
3	MINUTE (TIME)	See table **1002/1** which is a range [00 through 59] (2)

Table 2404 - PLAN ORIGINATOR AND NUMBER (5-36)

Related Documents: NONE

Definition: THE OFFICIAL IDENTIFIER OF A MILITARY ESTABLISHMENT WHICH IS RESPONSIBLE FOR A SPECIFIC OPERATION PLAN, AND THE IDENTIFICATION NUMBER ASSIGNED TO THAT SPECIFIC OPERATION PLAN.

Seq	Elemental FUD Name	Elemental Use
1	PLAN ORIGINATOR	See table **1029/2** which is an instructive entry (3-20)
2	BLANK SPACE CHARACTER	See table **1025/4** which is an instructive entry (1)
3	PLAN NUMBER	See table **1012/146** which is an instructive entry (1-15)

Table 2501 - DATA RATE (4-16)

Related Documents: NONE.

Definition: THE RATE OF DATA TRANSMISSION OR RECEPTION OVER A COMMUNICATIONS LINK.

Seq	Elemental FUD Name	Elemental Use
1	CONTEXT QUANTITY, DECIMAL PT PERMITTED, 6 CHAR MAX	See table **1023/28** which is a range [0 through 999999.00000] (0 to 5 decimal places) (1-12)
2	UNIT OF DATA RATE MEASUREMENT	See table **1008/113** which is a coded item (3-4)

Table 6004 - INTERNET PROTOCOL (IP) ADDRESS, IPV4 (7-15)

Related Documents: None

Definition:

Seq	Elemental FUD Name	Elemental Use
1	INTERNET PROTOCOL (IP) ADDRESS OCTET	See table **1012/700** which is a range [0 through 255] (1-3)
2	DECIMAL POINT	See table **1025/3** which is a coded item (1)
3	INTERNET PROTOCOL (IP) ADDRESS OCTET	See table **1012/700** which is a range [0 through 255] (1-3)
4	DECIMAL POINT	See table **1025/3** which is a coded item (1)
5	INTERNET PROTOCOL (IP) ADDRESS OCTET	See table **1012/700** which is a range [0 through 255] (1-3)
6	DECIMAL POINT	See table **1025/3** which is a coded item (1)
7	INTERNET PROTOCOL (IP) ADDRESS OCTET	See table **1012/700** which is a range [0 through 255] (1-3)

GLOSSARY OF TERMS

ACRONYMS

ACIXS	Allied Communication Information Exchange System
ACL	Access Control List(s)
ACP	Allied Communications Publication
ADNS	Automated Digital Network System
ALE	Automatic Link Establishment
ARQ	Automatic Repeat Request
AS	Autonomous System
ASN	Autonomous System Number
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code Information Interchange
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Organisation
AUS	Australia
BER	Bit Error Rate
BERT	Bit Error Rate Test
BIND	Berkeley Internet Name Domain
BGP	Border Gateway Protocol
BLOS	Beyond Line of Sight
BPD	Boundary Protection Device
CA	Canada
CAP	Channel Access Processor
CAR	Committed Access Rate
CAS	Collaboration At Sea
CATF	Commander Amphibious Task Force
CBWFQ	Class Based Weighted Fair Queuing
CCEB	Combined Communications-Electronics Board
CCI	Controlled Cryptographic Item
CELP	Code Book Excited Linear Predictive

CENTRIXS	Combined Enterprise Regional Information Exchange System
CFE	CENTRIXS Four Eyes
CFLCC	Coalition Force Land Component Commander
CFMCC	Coalition Force Mobile Component Commander
CIDR	Classless Inter-Domain Routing
CIK	Crypto Ignition Key
CJTF	Commander Joint Task Force
CODS	Coalition Data Server
CONOPS	Concept of Operations
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
COWAN	Coalition Operations Wide Area Network
CQ	Custom Queuing
CRIU	CAP to Router Interface Unit
CST	COP Synchronization Tool
CSU	Crypto Support Unit
CT	Cipher Text
CTF	Commander Task Force
CTG	Commander Task Group
CWAN	Coalition Wide Area Network
CWC	Composite Warfare Commander
DAC	Discretionary Access Control
DAMA	Demand Assigned Multiple Access
DBS	Direct Broadcast Service
DCP	Distributed Collaborative Planning
DNS	Domain Name Service
DTD	Data Transfer Device
DVMRP	Distance Vector Multicast Routing Protocol
EKMS	Electronic Key Management System
ELOS	Extended Line of Sight

EMCON	Emission Control
EoS	Elements of Service
FF	Fire Fly
FIFO	First In, First Out
FOTC	Force Over The Horizon Track Coordinator
FTP	File Transfer Protocol
GBS	Global Broadcast System
GCCS-M	Global Command Control System – Mobile
GCTF-1	Global Coalition Task Force One
GEM	General Dynamics Encryptor Management
GOTS	Government off the Shelf
GUI	Graphical User Interface
HAG	High Assurance Guard
HDR	High Data Rate
HF	High Frequency
HIT	High Interest Track
HSD	High Speed Data
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Numbers Authority
ICE	Imagery Compression Engine
IDM	Information Dissemination Management
IDP	Information Dissemination Plan
IGMP	Internet Group Management Protocol
IIS	Internet Information Service
IM	Information Management
IMI	Information Management Infrastructure
IMAP	Internet Message Access Protocol
IMPP	Instant Message and Presence Protocol
INE	In-line Network Encryptors
INMARSAT	International Mobile Satellite Organisation

IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IWC	Information Warfare Commander
IXS	Information eXchange System
JCSS	Joint Command Support System (Australia)
JMUG	JMCIS Multicast Gateway
KMID	Key Management Identification
LAN	Local Area Network
LDAP	Light Directory Access Protocol
LES	Land Earth Station
LMD/KP	Local Management Device / Key Processor
LOS	Line of Sight
LSA	Link State Advertisements
MAC	Media Access Control
MAG	Mobile Air Group
MCAP	Medium Data Rate Channel Access Processor
MCOIN	Mobile Command Operations Information Network (Canada)
MDP	Multicast Dissemination Protocol
MDR	Medium Data Rate
METOC	Meteorological/Oceanographic
MFTP	Multicast File Transfer Protocol
MMF	Multi-National Marine Force
MNTG	Multi-National Naval Task Group
MOSPF	Multicast Open Shortest Path First
MPLS	Multi-Protocol Label Switching
MSAB	Multinational Security Accreditation Board
MSeG	Multicast Service Gateway
MSL	Multi- Security Levels
MTA	Message Transfer Agent
MTWAN	Mobile Tactical Wide Area Network

NBAR	Network-Based Application Recognition
NCW	Network Centric Warfare
NES	Network Encryption System
NM	Network Management
NNTP	Network News Transport Protocol
NOC	Network Operations Center
NRS	Naval Radio Station
NZ	New Zealand
OPCON	Operational Control
OPGEN	Operational General Messages
OPTASK	Operational Tasking Messages
OSI	Open System Interconnect
OSPF	Open Shortest Path First
OTCIXS	Officer in Tactical Command Information eXchange System
PAD	Packet Assembler Disassembler
PC	Personal Computer
PCM	Pulse Code Modulation
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PLAD	Plain Language Address Designator
P_MUL	Protocol Multicast
POP3	Post Office Protocol Version 3
PPK	Pre-Placed Keys
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PT	Plain Text
QOS	Quality of Service
RED	Random Early Drop
RIP	Routing Internet Protocol
RF	Radio Frequency
RP	Rendezvous Point

RSVP	Resource ReServation Protocol
RTF	Rich Text Format
RTT	Round-Trip Time
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network (United States)
SMG	Secure Mail Guard
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	SubNet Relay
SOPS	Standard Operating Procedures
TBS	Theatre Broadcast Systems
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEK	Transmission Encryption Key
TG	Task Group
TOIS	Technical Operating Instructions
TOS	Type Of Service
TTL	Time To Live
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UID	Unit Identifier
UK	United Kingdom
US	United States
USS	United States Mobile
VHF	Very High Frequency
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Dropping
Z	Cryptographic Device

ACP 200(D) Vol 2